MATH 553: Abstract Algebra Qualifying Exam Prep

Kale Stahl

Contents

Part I
Notes

1 Groups

Proposition 1.1. *If G is a simple group and $H \leq G$, then $|G| \Big| [G : H]!$.*

Lemma 1.1. *$N \trianglelefteq G$ if N and G/N are solvable, then G is solvable*

Lemma 1.2. *Every p-group is solvable.*

2 Rings

2.1 Integral Domains

Definition 2.1. *A ring R is an integral domain if*

(a) *R is commutative*

(b) *$1 \in R$, and $1 \neq 0$*

(c) *$ab = 0$ implies that $a = 0$ or $b = 0$*

Definition 2.2. *A ring R is a field if*

(a) *R is commutative*

(b) *$1 \in R$, and $1 \neq 0$*

(c) *For all $a \neq 0 \in R$, there exists $b \in R$ such that $ab = 1$.*

Proposition 2.1. *Every finite integral domain is a field.*

Proof. Take some $a \in R$. Consider $x \mapsto ax$ and $ax = ay$, which implies $a(x - y) = 0$ meaning either $a = 0$ or $x - y = 0$, and since $a \neq 0$ we have that $x = y$ and $1 = ab$ for some b $\square$

Proposition 2.2. *If R is a domain, then*

(a) $\deg p(x)q(x) = \deg p(x) + \deg q(x)$

(b) *$R[x]$ is a domain.*

(c) *The units of $R[x]$ are the units of R.*

Definition 2.3. *If R is an integral domain, we denote by $Q(R)$ (Field of fractions of R) the field*

$$Q(R) = \{(a, b) \in R \times R \setminus \{0\}/\sim\} \tag{2.1}$$

where $\overline{(a, b) \sim (c, d)} \leftrightarrow ad = bc$. We also have $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$ and $\overline{(a, b)} + \overline{(c, d)} = \overline{(ac, bd)}$. Then $\overline{(a, b)}^{-1} = \overline{(b, a)}$ for $\overline{(a, b)} \neq \overline{(0, 1)}$.

Lemma 2.1. *Suppose R is an integral domain. Then $R[x_1, \dots, x_n]$ is also an integral domain.*

Proof. It suffices to prove that $R[x]$ is also an integral domain. If

$$f = a_m x^m + \cdots + a_0, \quad a_m \neq 0 \tag{2.2}$$
$$g = b_n x^n + \dots b_0, \quad b_n \neq 0 \tag{2.3}$$

Then $fg = a_m b_n x^{m+n} + \dots$ but $a_m b_n \neq 0$ since R is an integral domain. So $R[x]$ has no zero divisors. $\square$

Proposition 2.3. *$R \to Q(R)$ is an example of a ring homomorphism which is an epimorphism without being surjective as a map.*

2.2 Euclidean Domains

Definition 2.4. *If I, J are ideals of a commutative ring R then*

- *$I \cap J$ is an ideal.*
- *$I + J = \{a + b : a \in I, b \in J\}$ is an ideal.*
- *$IJ = \{\sum_i a_i b_i : a_i \in I, b_i \in J\}$ is an ideal and $IJ \subset I \cap J$.*

Proposition 2.4. *Let $I \subseteq R$. Then*

(a) *$I = R$ if and only if I contains a unit.*

(b) *If R is commutative then R is a field if and only if $0, R$ are the only ideals.*

(c) *If R is a field and S is a ring and there is some ring homomorphism $f : R \to S$, then $f = 0$ or f is injective.*

Definition 2.5. *If $S \subset R$ is a subset $(S) = \{\sum_{s \in S} a_s s : a_s \in R\}$ is an ideal and is called the ideal generated by S. If $S = \{s\}$ then $(S) = (s)$ and is called a principal ideal.*

Proposition 2.5. *In a unital ring, every proper ideal is contained in a maximal ideal.*

Definition 2.6. *An ideal $p \subset R$ is a prime ideal if it satisfies the property*

$$xy \in P \implies x \in P \text{ or } y \in P \tag{2.4}$$

An ideal $M \subset R$ is a maximal ideal if $M \neq R$ and satisfies for every ideal I $M \subset I \implies I = M$ or R.

Theorem 2.1. ***(a)*** *P is prime if and only if R/P is an integral domain.*

(b) *M is a maximal ideal if and only if R/M is a field.*

Corollary 2.1.1. *If R is a unital domain, then maximal ideals are prime.*

Theorem 2.2. *Let R be commutative (not necessarily unit). Let $D \subset R$ which is closed under multiplication, does not contain a zero divisor, and does not contain 0. Then there is a commutative ring Q such that $R \subset Q$ and every element of D is a unit in Q. Moreover,*

(a) *Every element of Q is of the form $\frac{r}{d}$ for $r \in R$ and $d \in D$.*

(b) *Q is the smallest ring containing R in which all elements of D are units, i.e. if S is a commutative unital ring with identity and $\varphi : R \to S$ is an injective map such that $\varphi(d)$ is a unit for each $d \in D$, then there is an injective $\Phi : Q \to S$ such that*

$$\begin{tikzcd}
R \arrow[rr, hook] \arrow[dr, hook, "\varphi"'] & & Q \arrow[dl, "\Phi"] \\
& S &
\end{tikzcd}$$

Definition 2.7. *$I, J \subset R$ we say that I, J are coprime or comaximal if and only if $I + J = R$*

Theorem 2.3 (Chinese Remainder Theorem)**.** *Let $A_1, \ldots, A_k \subset R$ such that A_i, A_j are comaximal for $i \neq j$. The map*

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \tag{2.5}$$

has kernel $A_1 \cap \cdots \cap A_k$.

Definition 2.8. *A function $N : R \to \mathbb{N}$ with $N(0) = 0$ is called a norm on R. If $N(0) > 0$ for all $a \neq 0$, then N is a positive norm.*

Definition 2.9. *The integral domain R is a euclidean domain if it admits a norm N such that for all a, b with $b \neq 0$ there are q and r such that*

$$a = bq + r \tag{2.6}$$

Where $r = 0$ or $N(r) < N(p)$.

Proposition 2.6. *Every Ideal in a Euclidean domain is principal. More specifically, $I \subset R$ then $I = (d)$ for $d \in I$ with minimal norm.*

Proof. If $I = 0$, then we are done, so let $I \neq 0$ and take d as above. $(d) \subseteq I$, so let $a \in I$. There exists some q, r, such that $a = qd + r$, $r = a - qd$ and $r = 0$. Then we are finished. ☐

Definition 2.10. *Let $b \neq 0$.*

(a) *$b|a$ implies that $a = bx$ for some x.*

(b) *d is a GCD for a, b written as $d = (a, b)$ if and only if*

  (i) *$d|a$ and $d|b$*

  (ii) *If $d'|a$ and $d'|b$ then $d'|d$.*

Proposition 2.7. *$((a, b))$ is the unique smallest principal ideal containing a and b.*

Proposition 2.8. *Let R be a domain. Then if $(d) = (d')$ for some $d, d' \neq 0$, then $d = ud'$ for u a unit.*

Theorem 2.4. *Let R be a Euclidean domain, $a, b \in R$ be nonzero. Then the Euclidean Algorithm yields*

$$a = q_0 b + r_0 \tag{2.7}$$
$$b = q_1 r_0 + r_1 \tag{2.8}$$
$$\vdots$$
$$r_{n-1} = q_{n+1} r_n \tag{2.9}$$

Then

(a) *$r_n = (a, b)$.*

(b) *$r_n = ax + by$*

2.3 Principal Ideal Domains

Theorem 2.5. *If R is a Principal Ideal Domain, then every irreducible element is prime.*

Proposition 2.9. *Let R be a PID and $a, b \in R \setminus \{0\}$. Then $(a, b) = (d)$ for some d.*

(a) *$d = (a, b)$*

(b) *$d = ax + by$ for $x, y \in R$.*

(c) *d is unique up to unit multiplication.*

Proposition 2.10. *Every nonzero prime ideal in a PID R, is a maximal ideal. Moreover, If $R[x]$ is a PID, then R is a field.*

Theorem 2.6. *Suppose R is a PID and $a \in R$. Then the following are equivalent:*

(i) *a is irreducible*

(ii) *a is prime*

(iii) *(a) is prime*

(iv) *(a) is maximal*

2.4 Unique Factorization Domains

Theorem 2.7. *Every PID is a Unique Factorization Domain.*

Proof. If r is a unit, then r is irreducible and we are finished. We claim that $(r) \subset (p_1) \subseteq (p_{11}) \subset (p_{111}) \subset \dots$ cannot happen. This is because if $I_1 \subseteq I_2 \subseteq \dots$, then $I = \bigcup I_n$ meaning $(a) = I$ and $a_k \in I_k$ implying $(a) \subseteq I_k \subseteq I$. For uniequeness we proceed by induction on n. □

Definition 2.11. *Let R be a domain.*

(a) *Suppose $r \in R$ is not a unit and is nonzero. Then r is irreducible if and only if $r = ab$ implies a or b is a unit. Otherwise, it is reducible.*

(b) *An element $p \in R$ is prime if and only if (p) is prime if and only if $p|ab$ implies $p|a$ or $p|b$.*

(c) *a and b are associates if and only if they differ by a unit.*

Theorem 2.8. *If R is a UFD, then $R[x]$ is also a UFD.*

Corollary 2.8.1. *R is a UFD implies that $R[x_1, x_2, \dots x_n]$ is also a UFD.*

Definition 2.12. *For $R = \mathbb{Z}$, $f \in \mathbb{Z}[x]$, $f \neq 0$ is a primitive if gcd(coefficients of f) $= 1$*

Proposition 2.11. *Suppose $f \in \mathbb{Q}[x]$, $f \neq 0$. Then there exists $c \in \mathbb{Q}$, $f_0 \in \mathbb{Z}[x]$ such that $f = cf_0$ with f_0 primitive. Up to multiplication with units, f_0 and c are uniquely defined. Moreover, $f \in \mathbb{Z}[x]$ if and only if $c \in \mathbb{Z}$. We call c the content of f.*

Theorem 2.9 (Gauss Lemma)**.** *Let R be a UFF, F the field of fractions of R. Let $P(x) \in R[x]$. If $P(x)$ is reducible in $F[x]$ then it is reducible in $R[x]$.*

Corollary 2.9.1. *Suppose $f \in \mathbb{Z}[x]$ is primitive and $g \in \mathbb{Z}[x]$. If $f|g$ in $\mathbb{Q}[x]$, then $f|g$ in $\mathbb{Z}[x]$*

Corollary 2.9.2. *$f \in \mathbb{Z}[x]$ primitive and f is irreducible over $\mathbb{Z}[x]$ then f is irreducible over $\mathbb{Q}[x]$.*

Corollary 2.9.3. *If the GCD of the coefficients of $P(x)$ is 1, then $P(x)$ is reducible in $F[x]$ if and only if $P(x)$ is reducible in $R[x]$*

Theorem 2.10. *$R[x]$ is a UFD if and only if R is a UFD.*

Proposition 2.12. *Let $I \subset R$, $P(x) \in R[x]$ be nonconstant and monic. Then if $P(x)$ is reducible in $R[x]$, $\overline{P(x)}$ is reducible in $(R/I)[x]$.*

Theorem 2.11. *$f \in \mathbb{Z}[x]$ is irreducible if and only if either*

(a) *$f = c$ where $c \in \mathbb{Z}$ is prime.*

(b) *f is primitive and irreducible in $\mathbb{Q}[x]$.*

Theorem 2.12. *Every irreducible in $\mathbb{Z}[x]$ is a prime.*

3 Modules

Definition 3.1. *Let A be a commutative ring. An A-module M is an abelian group $M = (M, \oplus, 0)$ along with a map $\odot : A \times M \to M$ satisfying*

(i) $c \odot (d \odot \alpha) = (cd) \odot \alpha$

(ii) $c \odot (\alpha \otimes \beta) = c \odot \alpha \oplus c \odot \beta$

(iii) $c + d \odot \alpha = c \odot \alpha \oplus d \odot \alpha$

(iv) $I \odot \alpha = \alpha$

Definition 3.2. *If M and N are A-modules then $f : M \to N$ is a homomorphism.*

Definition 3.3. *N submodule of M and $B \subset N$. We say that B is a basis of N if*

(i) *B is linearly independent.*

(ii) *$span(B) = N$*

3.1 Free Modules

Definition 3.4. *M is a free A-module if it has a basis.*

Theorem 3.1. *Any two bases of a free A-module have the same cardinality.*

Definition 3.5. *We say that M is a direct sum of the submodules N_i if $M \cong \bigoplus_i N_i$. In particular if N_1, N_2 are submodules of M, $M = N_1 \oplus N_2$ if and only if $M = N_1 + N_2$, and $N_1 \cap N_2 = 0$.*

Unlike in vector spaces, if $N \subset M$ is a submodule then there might not exist $N' \subset M$ such that $M = N \oplus N'$. If such an N' exists, we call N' a complementary submodule of N.

Definition 3.6. *If N is a submodule of M such that there exists $N' \subset M$ such that $M = N \oplus N'$, then N is called a direct factor of M.*

Definition 3.7. *We say that $p \in \mathrm{End}\,(M) = \hom(M, M)$ is a projector if $p \circ p = p$.*

Theorem 3.2. *If N is a submodule of M, then N is a direct factor of M if and only if there exists a projector $p \in \mathrm{End}\,(M)$ such that $N = p(M)$.*

Proof. Suppose $p \in \mathrm{End}\,(M)$ is a projector such that $N = p(M)$. Then $M = P(M)+(1-P)M$. Suppose $\alpha \in p(M)\cap(1-P)M$. Then

$$\alpha = p(\beta) = (1-p)(\gamma) = \gamma - p(\gamma) \tag{3.1}$$

Applying p to both sides we get

$$p(\beta) = p(\gamma) - p(\gamma) = 0 \implies \alpha = 0 \tag{3.2}$$

So $M = p(M) \oplus (1-p)M$. Conversely if N is a direct factor built complementary N then every $\alpha \in M$ can be expressed uniquely as $\alpha = \beta + \gamma$, $\beta \in N, \gamma \in N'$. □

Theorem 3.3. *If A is a PID. Then every submodule of a finite A-module is free.*

Proof. Suppose L is a free A-module and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L and M submodule of L. Let $M_i = M \cap \mathrm{Span}\,(\alpha_1, \ldots, \alpha_n)$. Let $P_i : L \to A$ denote the coordinate function. $P_i(M_i)$ is an ideal of A, and $P_i(M_i) = (d_i)$, $d_i \in A$. So then there exists $\beta_i \in M_i$ such that $P_i(\beta_i) = d_i$. Let $N_i = \mathrm{Span}\,(\beta_i)$. We claim that for $i = 1, \ldots, n$, $M_i = \sum N_i$ and the sum is direct. Suppose we know this for $M_h = \sum_{j \le h} N_j$ for all $h < k$. $\alpha \in M_k$. From definition of N_k, there exists $\beta \in N_k$ such that $P_k(\alpha) = P_k(\beta)$ since $N_k \cong P_k(M_k)$ so $P_k(\alpha - \beta) = 0$ which implies $\alpha - \beta \in M_{k-1} = M \cap \mathrm{Span}\,(\alpha_1, \ldots, \alpha_{k-1})$. By induction $\alpha - \beta \in \sum_{j \le k} N_y$, $\beta \in N_k$. So, $\alpha \in \sum_{j \le k} N_j$ and $M_k = \sum_{j \le k} N_j$. You get the idea. □

Theorem 3.4. *Suppose A is a PID and L a free A-module and M submodule of L (necessarily free) of rank n. Then there exists a basis B of L and $\beta_1, \ldots, \beta_n \in B$ and $a_1, \ldots a_n$ such that $\{a_1\beta_1, \ldots a_n\beta_n\}$ is a basis of M and $a_1|a_2|\ldots|a_n$.*
Moreover, $M' = \mathrm{Span}\,(\beta_1, \ldots, \beta_n)$ and $(a_1) \supset (a_2) \subset \cdots \supset (a_n)$ and uniquely determined by L, M.
Moremoreover, if $(L/M)_{tor} \cong \bigoplus_i^n A/(a_i)$ and $L/M \cong (L/M)_{tor} \oplus$ (Free module).

4 Fields

Theorem 4.1. *Suppose K is a field and G is a finite subgroup of K. Then G is cyclic.*

Definition 4.1. *$k \subset K$ is a field. K is an extension of k. K is a k-vector space. $\dim_k K = [K : K]$ the degree of the extension K/k.*

Proposition 4.1. *$k \subset K \subset L$. Then*

$$[L : k] = [L : K][K : k] \tag{4.1}$$

Definition 4.2. *Suppose K/k is a field extension and $\alpha \in K$. We say that α is algebraic over k if there exists some $f \in k[x]$ such that $f(\alpha) = 0$. Otherwise α is transcendental over k.*

Proposition 4.2. *Every finite field extension is algebraic.*

Definition 4.3. *K/k is an algebraic extension if every $\alpha \in K$ is algebraic over k.*

Theorem 4.2. *$[K : k] < \infty$, then K/k is algebraic.*

Lemma 4.1. *Suppose k/K is a field extension and $\alpha \in K$ is algebraic over k. Let $\varphi_\alpha : k[x] \to K$ to be the evaluation homomorphism at α, $f \mapsto f(\alpha)$. Then*

$$\operatorname{im}\varphi_\alpha = k(\alpha) \tag{4.2}$$
$$\ker\varphi_\alpha = (\operatorname{Irr}(\alpha, k)) \tag{4.3}$$

Where $\operatorname{Irr}(\alpha, k)$ is the unique monic polynomial generating $\ker\varphi_\alpha$.

Theorem 4.3. *If k is a field and $f \in k[x]$, f is not a non-zero constant. Then there exists K/k and $\alpha \in K$ such that $f(\alpha) = 0$ in K.*

Theorem 4.4. *If k is a field and $f \in k[x]$, then any two splitting fields are isomorphic.*

Definition 4.4. *Suppose $S \subset k[x]$ is a set of polynomials and $\overline{k}$ on algebraic closure of k. Then $k \subset K \subset \overline{k}$ and is a splitting field of S if K contains all the roots of each $f \in S$, and K is generated by these roots.*

Theorem 4.5. *Suppose $\overline{k}$ is an algebraic closure of K and K, $k \subset K \subset \overline{k}$ is a splitting field. Then any embedding*

$$\sigma : K \to \overline{k}, \qquad \sigma|_K = I_k \tag{4.4}$$

induces an automorphism of K.

Theorem 4.6. *$f \in k[x]$ has simple roots of and only if $(f, f') = (1)$.*

Corollary 4.6.1. *If char $k = 0$ and $f \neq 0$ is irreducible, then f has simple roots.*

Definition 4.5. *Suppose k is a field $\operatorname{char} k = p$*

$$\varphi_p : k \to k, \quad \alpha \mapsto \alpha^p \qquad \textit{(Frobenius Map)} \tag{4.5}$$

Proposition 4.3. *Suppose k is a field with $\operatorname{char} k = p$.*

$$(\alpha + \beta)^p = \alpha^p + \beta^p \tag{4.6}$$

Definition 4.6. *An irreducible polynomial $f \in k[x]$ is separable if all its roots are simple.*

Proposition 4.4. *Suppose $\operatorname{char} k = p$ and f is irreducible and not separable. Then there exists irreducible $g \in k[x]$ such that $f = g(x^p)$.*

Proposition 4.5. *Let $\operatorname{char} k = p$ and $a \in k$. Then $x^p - a$ is either irreducible or a pth power.*

Definition 4.7. *k is perfect if every irreducible is separable.*

Proposition 4.6. *$\operatorname{char} k = 0$, then k is perfect.*

Proposition 4.7. *$\operatorname{char} k = p$. Then k is perfect if and only if $\varphi_p(k) = k^p = k$.*

Corollary 4.6.2. *All finite fields are perfect.*

Definition 4.8. *K/k is a field extension. $\alpha \in K$ is separable over k, if $\operatorname{Irr}(\alpha, k)$ is separable. K/k is separable if every $\alpha \in K$ is separable.*

4.1 Galois Theory

Definition 4.9 (Galois Extension)**.** *K/k is a Galois Extension if it is normal and separable.*

Part II
Past Exams

Exam 1: January 2024 - Shahidi

Problem 1.1: Solvability

Let p, q and r be three distinct prime numbers iwth $p > qr$. Let n be a positive integer. Show that every group G of order $O(G) = p^n qr$ is solvable. Conclude that every group of order 294 or 1210 is solvable.

Solution to Problem 1.1:

□

Problem 1.2: Polynomials of prime order

Let q be a prime number and let

$$f_q(x) = x^{q-1} + x^{q-2} + \cdots + 1 \tag{1.2.1}$$

(a) Suppose a prime number p divides $f_q(a)$ for some integer a. Prove that either $p = q$ or $p \equiv 1 \mod q$.

(b) Prove there are infinitely many primes of the form $qb + 1$, where b is an integer.

Solution to Problem 1.2:

(a)

(b)

□

Problem 1.3: Irreducibles on Euclidean Domain

(a) Prove that $A = \mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

(b) Show that

$$A/(3 + 2\sqrt{-2}) \cong \mathbb{Z}/17\mathbb{Z} : \mathbb{F}_1 7 \tag{1.3.1}$$

(c) Show that $x^4 + 3$ is irreducible over $\mathbb{F}_1 7$ and conclude that

$$f(x) = x^4 - 170x + 9 + 4\sqrt{-2} \in A[x] \tag{1.3.2}$$

is irreducible over $A[x]$.

Solution to Problem 1.3:

(a)

(b)

(c)

□

Problem 1.4

Let n be an integer and let

$$f(x) = x^3 - (n-3)x^2 - nx - 1 \tag{1.4.1}$$

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}[x]$.

(b) Show that if a is a root of $f(x)$ then $-1/(a+1)$ is also a root of $f(x)$.

(c) Let K be the splitting field of $f(x)$ over Q. Shoe that the Galois extension over $K/\mathbb{Q}$ is cyclic of order 3. Conclude that all the roots of $f(x) = 0$ are real.

Solution to Problem 1.4:

$\square$

Problem 1.5

Solution to Problem 1.5:

$\square$

Problem 1.6

Solution to Problem 1.6:

$\square$

Problem 1.7

Solution to Problem 1.7:

$\square$

Exam 2: August 2024

Problem 2.1

(a) Prove that $x^3 - x - 1$is irreducible over $\mathbb{Z}$.

(b) Prove that $x + 1$ and $x^3 - x - 1$ are relatively prime in $\mathbb{Z}[x]$ i.e. theu generate the whole ring.

(c) Give a simpler interpretation of $\mathbb{Z}[x]/(x + 1)(x^3 - x - 1)$

Solution to Problem 2.1:

□

Problem 2.2

If $n \in \mathbb{N}$, $n \geq 1$. Prove that $f_n(x) = (x - 1)(x - 2) \ldots (x - n) - 1$ is irreducible over $\mathbb{Z}$. Is it irreducible over $\mathbb{Q}$?

Solution to Problem 2.2:

□

Exam 3: August 2022 - Shahidi

Problem 3.1

(a) Show that every solvable group has a non-trivial normal abelian subgroup.

(b) Let G be a group and denote $Aut(G)$ the group of its automorphisms. Assume $Aut(G)$ is solvable. Prove that G is solvable.

Solution to Problem 3.1:

$\square$

Problem 3.2: Classifying all groups of order pq

Let p and q be two prime numbers with $p < q$. Let G be a group of order pq.

(a) Assume p does not divide $q - 1$. Show that G is cyclic which is a direct product of a q-Sylow subgroup Q and a p-Sylow subgroup P of G.

(b) Assume $p|q - 1$ abd G is not cyclic. Conclude that in this case G is non-abelian and is a semi-direct profuct of a q-Sylow subgroup Q and a p-Sylow subgroupf P of G, but not their direct product.

(c) Let p and q be two primes as above with $p|q-1$. Let P and Q be the cyclic groupds of orders p and q respectively. Show that all the semi-direct products $Q \rtimes_\varphi P$ where $\varphi : P \to Aut(Q)$ and non-trivial homomorphisms, are isomorphic. You may assume the fact that finite subgroups of the multiplication groupd of a field are cyclic.

Solution to Problem 3.2:

$\square$

Exam 4: August 2013

Problem 4.1

In which of the following rings is every ideal principal?

(a) $\mathbb{Z}/4\mathbb{Z}$

(b) $\mathbb{Z} \oplus \mathbb{Z}$

(c) $\mathbb{Z}/4\mathbb{Z}[x]$

(d) $\mathbb{Z}/6\mathbb{Z}[x]$

Solution to Problem 4.1:

$\square$

Part III
Extra Problems

Exam 5: Basu Practice Final Spring 2025

Problem 5.1: Conjugacy Classes

Let G be a finite group.

(a) What is the conjugacy class of an element $g \in G$?

(b) Prove that the number of elements in a conjugacy class divides the order G.

(c) If G has only 2 conjugacy classes, prove that G has order 2.

Solution to Problem 5.1:

(a) The conjugacy class G_g of g is defined as

$$C_g = \{x \in G : xgx^{-1}\} \tag{5.1.1}$$

(b) We note that

$$|C_g| = [G : C_G(g)] \tag{5.1.2}$$

where $C_G(g)$ is the centralizer of g. Since the centralizer is a subgroup of G, we can apply Lagrange's Theorem to see

$$|G| = |C_G(g)|[G : C_G(g)] = |C_G(g)||C_g| \tag{5.1.3}$$

So then the order of a conjugacy class divides the order of G.

(c) Let $x \in G$ such that $x \neq e$, and let C_x be the conjugacy class of x. Trivially we must have that $C_e = \{e\}$, which implies that if $|G| = n$, then $|C_x| = n - 1$. By the previous problem, we can apply lagranges theorem to see that $n - 1|n$, which means that only $n = 2$.

$\square$

Problem 5.2: Group is abelian if there is an automorphism for every element

Let G be a finite group. Suppose that for every $a, b \in G$ distinct from the identity, there is an automorphism of G taking a to b. Prove that G is abelian.

Solution to Problem 5.2: Since G is finite, every element of G has finite order. Since any two elements of $G \setminus \{e\}$ are related by an automorphism of G, all elements must have the same order, say q. Since all powers of an element of $G \setminus \{e\}$ have either order q or 1, then q must be prime. By Sylow's Theorem, the order of G is a power of q. Thus, $Z(G)$ contains an element other than e, meaning $Z(G) = G$ which means G is abelian. $\square$

Problem 5.3: Intersection of subgroups has finite index

Let G be a group and H, K subgroups of G such that H has a finite index in G. Prove that $K \cap H$ has a finite index in K.

Solution to Problem 5.3: Since $H \cap K$ is a subgroup of both H and K, both $[K : H \cap K]$ and $[H : H \cap K]$ are well defined. We see

$$[G : H] = [G : K]K : H = [G : K][K : K \cap H][K \cap H : H] \tag{5.3.1}$$

Since $[G : H]$ is finite, and $[K \cap H : H]$ is finite, then $[K : K \cap H]$ is also finite. ☐

Problem 5.4: Cyclic if only one subgroup shares order

Let G be a finite group of order n with the property that for each d such that $d|n$, there is at most one subgroup of G of order d. Prove that G is cyclic.

Solution to Problem 5.4: Let D br the set of all orders of elements of G. If $a \in G$ has order $|a| = d$, then (a) is the unique subgroup in G of order d and so all elements of order d must be in (a). It follows that there are exactly $\varphi(d)$ elements in G of order $d \in D$. We then see

$$n = \sum_{d \in D} \varphi(d) \leq \sum_{d|n} = n \tag{5.4.1}$$

So then $n \in D$ and G is cyclic. ☐

Problem 5.5: Group is cyclic if it has subgroup of order 2

Let p be an odd prime and G a group of order $2p$. Suppose that G has a normal subgroup of order 2. Prove that G is cyclic.

Solution to Problem 5.5: We know that $[N : G] = p$, so then $|G/N| = p$ and is cyclic. Let gN generate G/N. In particular, we have $g^p N = (gN)^p = N$. Suppose G is not cyclic. Then since any abelian group of order 2 is cyclic, then the order of g must be p. Since N is normal in G, gxg^{-1}, the order of gx is $2p$ so G is cyclic. ☐

Problem 5.6: Finding Galois Group

Let p be an odd prime number and $\varphi_p = X^{p-1} + \cdots + 1 \in \mathbb{Q}[X]$. Prove that $K = \mathbb{Q}[X]/(\varphi_p)$ is a splitting field of φ_p and $K/\mathbb{Q}$ is a Galois extension. What is the Galois group of the extension $K/\mathbb{Q}$?

Solution to Problem 5.6:

1. Roots of $\varphi_p(X)$

Let ζ_p be a primitive p-th root of unity, i.e., $\zeta_p = e^{2\pi i/p}$. Then the roots of the polynomial $\varphi_p(X)$ are exactly the primitive p-th roots of unity:

$$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}.$$

Therefore, the minimal polynomial of ζ_p over $\mathbb{Q}$ is $\varphi_p(X)$, which is irreducible in $\mathbb{Q}[X]$.

2. The field K

The quotient ring

$$K = \mathbb{Q}[X]/(\varphi_p)$$

is a field because $\varphi_p(X)$ is irreducible in $\mathbb{Q}[X]$. Moreover, K is isomorphic to the number field $\mathbb{Q}(\zeta_p)$ via the isomorphism

$$\mathbb{Q}[X]/(\varphi_p) \cong \mathbb{Q}(\zeta_p),$$

sending the class of X to ζ_p.

3. K is a splitting field of φ_p

Since $\varphi_p(X)$ splits completely in $\mathbb{Q}(\zeta_p)$, and all of its roots are in $\mathbb{Q}(\zeta_p)$, the field $K = \mathbb{Q}(\zeta_p)$ is the splitting field of $\varphi_p(X)$ over $\mathbb{Q}$.

4. $K/\mathbb{Q}$ is a Galois extension

An extension is Galois if it is both normal and separable. Since $\mathbb{Q}$ has characteristic 0, all field extensions are separable. Also, $K = \mathbb{Q}(\zeta_p)$ is the splitting field of a separable polynomial $\varphi_p(X)$, hence $K/\mathbb{Q}$ is normal. Therefore, $K/\mathbb{Q}$ is Galois.

5. The Galois group

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is isomorphic to the group of units of the ring $\mathbb{Z}/p\mathbb{Z}$, i.e.,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times.$$

This group has order $\varphi(p) = p - 1$ and is cyclic, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime p.
The isomorphism is given by sending a Galois automorphism σ to the integer $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\sigma(\zeta_p) = \zeta_p^a$.

Conclusion

The field $K = \mathbb{Q}[X]/(\varphi_p) \cong \mathbb{Q}(\zeta_p)$ is the splitting field of $\varphi_p(X)$ over $\mathbb{Q}$. The extension $K/\mathbb{Q}$ is Galois, and the Galois group is

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}_{p-1}.$$

□

Problem 5.7: Every subgroup of a field is cyclic

Prove that every finite subgroup of the multiplicative group of a field is cyclic.

Solution to Problem 5.7: Let G be the multiplicative group of a finite field with order n. Let $x \in G$ such that $|x| = d$. Let H be the subgroup of G generated by x. If $G = H$, we are done, so suppose otherwise. Then there exists $y \in G \setminus H$ with $|y| = m$ and $\ell = lcm(d, m)$. Suppose $d = \ell$. Then $m|d$ and $y^d = 1$. This contradicts the fact that the number of solutions to $X^d - 1 = 0$ is less than or equal to d, meaning $d < \ell$. By a theorem in the book, there exists an element $z \in G$ such that $|z| = \ell$. We can repeat this process until we find a generator of G, which means that H is cyclic. □

Problem 5.8: $\mathbb{Z}[X]$ is a UFD

Prove that the ring $\mathbb{Z}[X]$ is a unique factorization domain.

Solution to Problem 5.8: We prove that $\mathbb{Z}[X]$ is a UFD by using the following facts:

1. A principal ideal domain (PID) is a UFD.

2. The ring $\mathbb{Z}$ is a principal ideal domain, hence a UFD.
3. If R is a UFD, then $R[X]$ is also a UFD.

Now, let us apply these facts:

- Since $\mathbb{Z}$ is a principal ideal domain, it is a UFD.
- By a standard result in commutative algebra, if R is a UFD, then the polynomial ring $R[X]$ is also a UFD.
- Therefore, since $\mathbb{Z}$ is a UFD, the ring $\mathbb{Z}[X]$ is also a UFD.

Hence, every non-zero, non-unit element in $\mathbb{Z}[X]$ can be written as a product of irreducible elements, and this factorization is unique up to order and units. $\square$

Problem 5.9: Splitting fields

Let k be a field and $f \in k[X]$ and let $\deg(f) = n$. Prove that if K is a splitting field of f then $[K : k]$ divides $n!$.

Solution to Problem 5.9: Let $n_1, n_2, \ldots, n_k$ be the degrees of the irreducible factors of f. Then $\sum_i n_i = n$. We know this holds for all irreducibles, so

$$[K : k] | n_1! n_2! \ldots n_k! \tag{5.9.1}$$

However, the coeffificent

$$\binom{n}{n_1, n_2, \ldots n_k} = \frac{n!}{n_1! n_2! \ldots n_k!} \tag{5.9.2}$$

Is the number of ways to choose to separate n things into k groups of sizes $n_1, \ldots, n_k$ and as such must be an integer. So,

$$n! = j(n_1! n_2! \ldots n_k!) \tag{5.9.3}$$

for some $j \in \mathbb{Z}$, so then $[K : k] | n!$ and we are done. $\square$

Problem 5.10: Counting subgroups of S_p

Let p be a prime and S_p denote the symmetric group on p elements.

(a) What is the order of a p-Sylow subgroup of S_p?

(b) What is the number of p-Sylow subgroups in S_p?

(c) Deduce that $(p-1)! \equiv -1 \mod p$.

Solution to Problem 5.10:

(a) The order of any p subgroup is p. Since p is defined to be the largest prime power that divides the order of S_p, which is always p since $|S_p| = p!$.

(b) All of the elements of order p consist of a p-cycle of the first p natural numbers, so there are exactly $(p-1)!$ elements of order p. Each subgroup of order p contains $p-1$ elements of order p (the non-identity elements), so the intersection of any two subgroups is trivial, so the number of subgroups of order p is

$$\frac{(p-1)!}{p-1} = (p-2)! \tag{5.10.1}$$

(c) By Sylow's Third theorem, part **(b)** implies that

$$(p-2)! \equiv 1 \mod p \tag{5.10.2}$$

multiplying both sides by $(p-1)$ gives

$$(p-1)! \equiv p-1 \equiv 1 \mod p \tag{5.10.3}$$

$\square$

Problem 5.11: Composition of normal field extensions

Prove or disprove: The composition of any two normal extension of a field k is normal.

Solution to Problem 5.11: This is not true, a counterexample would be

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \tag{5.11.1}$$

$\square$

Problem 5.12: Group with order 2 is abelian

Prove that a group G in which every element is of order 2 is abelian.

Solution to Problem 5.12: Since every element has order 2, $a^{-1} = a$ for all $a \in G$, so

$$[a,b] = aba^{-1}b^{-1} = abab = (ab)^2 = e \tag{5.12.1}$$

So the group is abelian. $\square$

Problem 5.13: Union of conjugates is a subgroup

Prove that if H is a proper subgroup of a finite group G, then $\bigcup_{x\in G} x^{-1}Hx \neq G$.

Solution to Problem 5.13: Let G have order n, and since H is a proper subgroup, let $[G:H] = m > 1$. Let $N(H)$ be the normalizer of H in G, which contains H. As such, $[G:N(H)] \leq [G:H]$. We can let G act by conjugation, so then the orbit of G is the set of all conjugate subgroups. So the stabilizer fo G is exactly the normalizer $N(H)$, so then by the Orbit-Stabilizer Theorem, the number of all conjugate subgroups is equal to $[GN(H)]$. Each of these subgroups has cardinality $|H|$, and each has the indentity e, so the union has at most $1+[G:N(H)](|H|-1)$ elements in the union. So

$$
\begin{aligned}
1 + [G : N(H)](|H| - 1) &\leq 1 + [G : H](|H| - 1) && (5.13.1)\\
&= 1 + |G| - m && (5.13.2)\\
&= |G| + (1 - m) && (5.13.3)\\
&< |G| && (5.13.4)
\end{aligned}
$$

since $m > 1$, so the union of conjugate subgroups is a proper subset and not the whole of G. □

Problem 5.14: Semidirect Product

Prove that if H and K are subgroups of finite index in a group G, and $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

Solution to Problem 5.14: From the textbook, we know that if $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = KH$. So then we know that

$$[G : H][H : H \cap K] = \frac{|G|}{|H|}\frac{|H|}{|H \cap K|} = \frac{|G|}{|H \cap K|}\frac{|K|}{|K|} = [G : K][K : H \cap K] \tag{5.14.1}$$

Since $[G : K]$ and $[G : H]$ are relatively prime, we know that $[G : H]$ must divide $[K : H \cap K]$. So then we get that $[G : H] = [K : H \cap K]$ and by our proposition we are finished. □

Problem 5.15: Not all elements are in the conjugate

Prove that if H is a proper subgroup of finite index in a group G (possibly infinite), then there exists $x \in G$ not belonging to any conjugate of H.

Solution to Problem 5.15: Let H be a proper subgroup of G with finite index $n = [G : H]$. We aim to show that there exists an element $x \in G$ such that $x \notin gHg^{-1}$ for any $g \in G$.
Let X be the set of left cosets of H in G, so $|X| = n < \infty$. Consider the action of G on X by left multiplication:

$$g \cdot aH = gaH \quad \text{for } g, a \in G.$$

This defines a group homomorphism

$$\varphi : G \to \mathrm{Sym}(X) \cong S_n,$$

where S_n is the symmetric group on n letters.
Let $K = \ker(\varphi)$. Then K is a normal subgroup of G contained in the intersection of all conjugates of H:

$$K \subseteq \bigcap_{g \in G} gHg^{-1}.$$

Moreover, since $\varphi(G) \leq S_n$, the image is finite, and thus the kernel K is of finite index in G (as the kernel of a homomorphism to a finite group).
Now, since H is a proper subgroup, the image $\varphi(G)$ is a nontrivial subgroup of S_n, hence K is a proper subgroup of G.
Assume for contradiction that every $x \in G$ lies in some conjugate of H, i.e.,

$$G = \bigcup_{g \in G} gHg^{-1}.$$

But there are only finitely many distinct conjugates of H (since $[G : H] < \infty$), say

$$G = \bigcup_{i=1}^{m} g_i H g_i^{-1}.$$

This expresses G as a finite union of proper subgroups.
However, a standard result in group theory (e.g., B.H. Neumann's theorem) states that a group cannot be expressed as a finite union of proper subgroups unless one of them is equal to the whole group. Therefore, this leads to a contradiction.
Hence, there must exist some element $x \in G$ such that $x \notin gHg^{-1}$ for any $g \in G$. $\square$

Problem 5.16: G/H **is cyclic and abelian**

Prove that if H is a subgroup contained in the center of a group G, then H is a normal subgroup. Moreover, if G/H is cyclic, prove that G is abelian.

Solution to Problem 5.16: If $H \subset Z(G)$ and $h \in H$, then $h \in Z(G)$, so for every $g \in G$, we have

$$g^{-1}hg = g^{-1}gh = eh = h \tag{5.16.1}$$

Since this works for any $h \in H$, we have that $g^{-1}Hg =$ and H is normal.
Since G/H is cyclic, say it is generated by $\langle gH \rangle$. Then for some $a, b \in G$, $a \in g^i H$ and $b \in g^j H$. Then for some $h_1, h_2 \in H$ we have

$$\begin{aligned} ab &= (g^i h_1)(g^j h_2) && (5.16.2)\\ &= g^{i+j} h_1 h_2 && (5.16.3)\\ &= g^j h_2 g^i h_1 && (5.16.4)\\ &= ba && (5.16.5) \end{aligned}$$

so then it is commutative. $\square$

Problem 5.17: **Indexes of Finite Groups**

Let G be a finite group and p the smallest prime that divides the order of G. Prove that a subgroup of index p in G is normal.

Solution to Problem 5.17: Let H be a subgroup of index p. Then G acts on the set of left cosets of G by left multiplication, $x(gH) = xgH$. This action induces a homomorphism from $G \to S_p$, of which whose , K is in H. Then G/K is isomrphic to a subgroup of S_p, and has order dividing $p!$. But it also has order dividing $|G|$, and since p is the smallest prime which does this, then $|G/K| = p$. We see

$$|G/K| = [G : K] = [G : H][H : K] = p[H : K] \tag{5.17.1}$$

so then $[H : K] = 1$, so $K = H$ and since K is normal, H is thus normal. $\square$

Problem 5.18: Orbit Stabilizer

Let G be a finite group acting on a finite set X. Prove that the number of orbits equals

$$\frac{1}{|G|}\sum_{g\in G}|Fix(g)| \tag{5.18.1}$$

where $Fix(g)$ is the set of elements of X which are fixed by the action of g.

Solution to Problem 5.18:

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}|Fix(g)| &= \frac{1}{|G|}\sum_{g\in G}|\{x\in X : gx = x\}| && (5.18.2)\\
&= \frac{1}{|G|}\sum_{x\in X}|\{g\in G : gx = x\}| && (5.18.3)\\
&= \frac{1}{|G|}\sum_{x\in X}|Stab(x)| && (5.18.4)\\
&= \frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|Orb(x)|} && (5.18.5)\\
&= \sum_{x\in X}\frac{1}{|Orb(x)|} && (5.18.6)\\
&= \sum_{Orb(x)\in X/G}\left(\sum_{x\in Orb(x)}\frac{1}{|Orb(x)|}\right) && (5.18.7)\\
&= \sum_{Orb(x)\in X/G} 1 && (5.18.8)\\
&= |X/G| && (5.18.9)
\end{aligned}$$

□

Problem 5.19: Proof of Burnside's Lemma

Let G be a finite group acting transitively on a set of cardinality at least 2. Prove that there exists $g \in G$ such that $Fix(g) = \emptyset$.

Solution to Problem 5.19: By Burnside's Lemma we have

$$|orb(G)| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)| = 1 \tag{5.19.1}$$

Since it is transitive, so it has exactly 1 orbit. However, since the number of fixed points for each element must be an integer, only one can be one. So then there exists at least 1 $g \in G$ that fixes no points. □

Problem 5.20: Proof of First Sylow Theorem

Define p-Sylow subgroups of finite group G and prove they always exist.

Solution to Problem 5.20: A p-Sylow subgroup is a subgroup of G in which all elements have an order of p^n for some n, and is maximal among all p-subgroups of G.
To prove they always exist, let $|G| = kp^n$ such that $p \not| k$. Let $\mathcal{S} = \{S \subseteq G : |S| = p^n\}$ which is the set of all subsets of G which have exactly p^n elements . Let $N = |\mathcal{S}|$. We know that

$$N = \binom{p^n k}{p^n} \equiv k \mod p \tag{5.20.1}$$

Let G act on $\mathcal{S}$ by the following:

$$\forall S \in \mathcal{S} : g * S = gS = \{x \in G : x = gs : s \in S\} \tag{5.20.2}$$

which means $g * S$ is the left coset of S by g which is a group action. Now, let $\mathcal{S}$ have r orbits under this action which partition $\mathcal{S}$, meaning

$$|\mathcal{S}| = |Orb(S_1)| + |Orb(S_2)| + \cdots + |Orb(S_r)| \tag{5.20.3}$$

If each orbit had length divisible by p, then $p|N$. But this cannot be the case, as $N \equiv k \mod p$, so at least one orbit has length which is not divisible by p. So then for some S, there is $|Orb(S)| = m : p \not| m$. Let $s \in S$. Then $Stab(S)s = S$ meaning $|Stab(S)| = |S| = p^n$ and since the stabilizer is a subgroup, they must always exist. $\square$

Problem 5.21: **Abelian if every Sylow is normal and abelian**

Suppose that G is a finite group such that every Sylow subgroup is normal and abelian. Show that G is abelian.

Solution to Problem 5.21: Let $x, y \in G$. We split into multiple cases.
Case 1: If x and y are in the same Sylow subgroup, and since they are all abelian, we clearly have $xy = yx$.
Case 2: If x, y are not in the same Sylow subgroup, then suppose that $x \in P$ and $y \in Q$, Sylow p and q subgroups respectively. Since P and Q are normal, we have

$$xyx^{-1}y^{-1} \in P \cap Q = \{e\} \tag{5.21.1}$$

Which implies $xy = yx$ meaning it is abelian.
Case 3: x, y are in no Sylow p subgroups. Then they are both the identity and clearly are abelian. $\square$

Problem 5.22: **Product Ideals**

Let R be a commutive ring and I, J ideals of R.

- **(a)** Define the ideals IJ, $I \cap J$, and $I + J$ and prove in case that they are ideals.
- **(b)** Prove that $IJ \subset I \cap J$.
- **(c)** Suppose R is a PID. Show that $IJ = I \cap J$ if and only if $I + J = R$.

Solution to Problem 5.22:

- **(a)** We see that

$$IJ = \{a_1 b_1 + \cdots + a_n b_n : n \in \mathbb{N}, a_i \in I, b_j \in J\} \tag{5.22.1}$$

We need to show first that IJ is a subring of R. After this, suppose that $r \in R$ and $a \in IJ$ where $a = i_1 j_1 + \cdots + i_n j_n$. Note that

$$ra = r(i_1 j_1 + i_2 j_2 + \cdots + i_n j_n) = ri_1 j_1 + ri_2 j_2 + \cdots + ri_n j_n \tag{5.22.2}$$

Since I is an ideal, then $ri_k \in I$, so then $ra \in IJ$ and IJ is a left ideal. Since R is commutative, it is also a right ideal.

(b) Clearly $IJ \subset I$ and $IJ \subset J$,

(c) We begin with the reverse direction. Suppose $I + J = R$. Then

$$\begin{aligned} I \cap J &= (I \cap J) \cdot R & (5.22.3)\\ &= (I \cap J) \cdot (I + J) & (5.22.4)\\ &= (I \cap J) \cdot I + (I \cap J) \cdot J & (5.22.5)\\ &\subset IJ + IJ & (5.22.6)\\ &= IJ & (5.22.7) \end{aligned}$$

This, combined with part **(b)**, gives us that $IJ = I \cap J$.
The reverse direction can be seen by supposing $IJ = I \cap J$. For the sake of contradiction, suppose $I + J \neq R$. Then there exists a maximal ideal $m \subset R$ with $I + J \subset m$.

□

Problem 5.23: Irreducibles in an Integral Domain

Let R be an integral domain.

(a) Define irreducible elements and prime elements of R.

(b) Prove that every prime element of R is irreducible.

Solution to Problem 5.23:

(a) An irreducible elemnt in an integral domain is a non-zero element that is not invertible (not a unit) and is not the product of two non-invertible elements. An element is prime if it is not zero or unit and whenever P divides ab, for some $a, b \in R$ then p divides a or p divides b.

(b) Let (p) be prime in R. Let $p = ab$. Clearly $ab \in (p)$ but (p) is prime, so either $a \in (p)$ or $b \in (p)$. Suppose WLOG, $a \in (p)$ then there is some $r \in R$ in $a = pr \implies p = prb$. By cancellation, $1 = rb$ thus since p is irreducible, b is a unit and p is prime.

□

Problem 5.24: Irreducibles in a PID

Let R be a PID and $a \in R$ such that $a \neq 0$ and a is not a unit. Prove that the following are equivalent:

(a) a is irreducible.

(b) a is prime.

(c) (a) is a prime ideal.

(d) (a) is a maximal ideal.

Solution to Problem 5.24: We prove the equivalence in a cycle: (a) ⇒ (d) ⇒ (c) ⇒ (b) ⇒ (a).

(a) ⇒ (d): Assume a is irreducible. Since R is a PID, all ideals are principal. We claim that (a) is maximal.
Let $(a) \subseteq (b) \subseteq R$ for some ideal (b). Then $a \in (b)$, so $a = br$ for some $r \in R$. Since a is irreducible, either b or r is a

unit.

- If r is a unit, then a and b are associates, so $(a) = (b)$.
- If b is a unit, then $(b) = R$, so $(a) \subseteq R$.

Therefore, there are no ideals strictly between (a) and R, so (a) is maximal.

(d) $\Rightarrow$ (c): Every maximal ideal in a commutative ring is a prime ideal. Therefore, if (a) is maximal, then it is also prime.

(c) $\Rightarrow$ (b): Suppose (a) is a prime ideal. We want to show that a is a prime element. Let $a \mid bc$ for some $b, c \in R$. Then $bc \in (a)$, so by primality of the ideal, either $b \in (a)$ or $c \in (a)$. Hence, $a \mid b$ or $a \mid c$. Thus, a is a prime element.

(b) $\Rightarrow$ (a): Suppose a is prime. We show a is irreducible.
Assume $a = bc$ for some $b, c \in R$. Since a is prime, it must divide b or c. Without loss of generality, assume $a \mid b$. Then $b = ad$ for some $d \in R$, and so:

$$a = bc = (ad)c = a(dc).$$

Canceling a (which is nonzero and not a zero divisor in an integral domain), we get $1 = dc$, so c is a unit. Therefore, a is irreducible.

Hence, all four statements are equivalent. $\square$

Problem 5.25: **Every PID is a UFD**

Prove that every PID is a UFD.

Solution to Problem 5.25: Let R be a PID and suppose that a nonzero element $a \in R$ can be written two separate ways as products of irreducibles such that

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{5.25.1}$$

where each p_i and q_j are irreducible in R and $s \geq r$. Then p_1 divides the product $q_1 \dots q_s$ and so p_1 divides some q_j for some j since p is prime. By reordering, we can suppose that $p_1 | q_1$, meaning $p_1 = u_1 q_1$ for some unit u_1 of R. Since q_1 and p_1 are both irreducible. Thus,

$$p_1 p_2 \dots p_r = u_1 p_1 q_2 \dots q_s \tag{5.25.2}$$

So then we get

$$1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s \tag{5.25.3}$$

Since none of the q_j are a unit, then $r = s$ and p_j is associated with q_j in some permutation. Thus, R is a unique factorization domain. $\square$

Exam 6: Misc. Book Problems

Problem 6.1: No Simple Groups

Prove that there are no simple groups of order

(a) 30

(b) 105

(c) 56

Solution to Problem 6.1:

(a) Let G be a simple group of order $30 = 2 \cdot 3 \cdot 5$. So By the Sylow theorems, we have

$$n_2 \equiv 1 \mod 2 \tag{6.1.1}$$
$$n_3 \equiv 1 \mod 3 \tag{6.1.2}$$
$$n_5 \equiv 1 \mod 5 \tag{6.1.3}$$

meaning

$$n_2 \in \{1, 3, 5, 15\} \tag{6.1.4}$$
$$n_3 \in \{1, 10\} \tag{6.1.5}$$
$$n_5 \in \{1, 6\} \tag{6.1.6}$$

We will proceed case by case. If $n_2 = 1$, then let $P \in \mathrm{Syl}_2(G)$. Since $n_2 = 1$, this implies that $P \trianglelefteq G$ meaning that $|P| = 2$ which is a contradiction as G is simple. Thus, $n_2 \neq 1$. The same argument holds for $n_3 = 1$ and $n_5 = 1$. So we are left with

$$n_2 \in \{3, 5, 15\} \tag{6.1.7}$$
$$n_3 = 10 \tag{6.1.8}$$
$$n_5 = 6 \tag{6.1.9}$$

Let $H_1, H_2, \dots H_6 \in \mathrm{Syl}_5(G)$. We know that $|H_i| = 5$. Clearly H_i has 4 elements of order 5, so

$$|H_i \cap H_j| \Big| |H_i| \implies |H_i \cap H_j| \Big| 5 \tag{6.1.10}$$

If $|H_i \cap H_j| = 5$, then $H_i \cap H_j = H_i$ which is a contradiction, meaning $H_i \cap H_j = 1$ for all $i \neq j$. This means that G has at least 24 elements of order 5, but since $n_3 + 24 = 34 > 30 = |G|$ this is impossible. Thus, there are no simple groups of order 30.

(b)

(c)

(d)

$\square$