UC Berkeley, Math 250A
Groups, Rings, and Fields

— — —

Coursework Selection
Felix Gotti

The content presented in this informal writing consists, mostly, of my solutions to some problems showing in tests or assignments I had while taking the graduate course Math 250A at UC Berkeley (Fall 2014). Also I propose solutions to other problems that, although were not part of the course, I solved as part of my coursework. I warn the reader about that most of the solutions provided might be improved a lot; they are just the best I could do. I don't claim any ownership of any of the ideas presented; this is mainly because even those solutions that apparently are mine, ultimately belong to my kind and excellent professors Alexandre Turull and Vera Serganova, when are not a subconscious reproduction of techniques showed in Algebra by Serge Lang and/or Algebra by Thomas Hungerford. On the other hand, I claim full ownership of each of the potential existing errors. If the reader finds mistakes or have questions, please don't hesitate to email me at felixgotti@berkeley.edu. I will greatly appreciate your feedback. Having said this, I hope the small set of problems presented can be useful to the reader.

---

1 Group Theory

Problem 1. *Let G be an abelian subgroup of the symmetric group S_n and $p_1, \dots, p_k$ be all prime divisors of $|G|$. Prove that $p_1 + \dots + p_k \le n$.*

Solution: Suppose, by way of contradiction, that $p_1 + \dots + p_k > n$. Since p_i is a prime dividing $|G|$, the group G must have an element of order p_i. Therefore, for each i, G contains an element σ_i whose cycle-type decomposition is the product of p_i-cycles. For each j, denote by M_j the set of elements of $J_n = \{1, \dots, n\}$ that are not fixed by σ_j. Since G is abelian M_i and M_j are disjoint for $i \ne j$. The fact that $|M_j| \ge p_j$ implies that

$$|J_n| \ge |M_1| + \dots + |M_k| \ge p_1 + \dots + p_k > n;$$

which is a contradiction. Hence $p_1 + \dots + p_k \le n$.

■

Problem 2. *Let G be a finite group operating on a finite set S. For a fixed $x \in G$ define $f(x)$ as the number of elements $s \in S$ such that $xs = s$. Prove that the number of orbits of G in S is equal to*

$$\frac{1}{|G|} \sum_{x \in G} f(x).$$

Solution: Consider the set $A = \{(x, s) \in G \times S \mid xs = s\}$. We denote the orbit of $s \in S$ by $\mathcal{C}_s$. Note the $|A| = \sum_{x \in G} f(x)$. On the other hand, by the Orbit-Stabilizer theorem,

$$|A| = \sum_{s \in S} |\text{Stab}(s)| = \sum_{s \in S} \frac{|G|}{|\mathcal{C}_s|} = |G| \sum_{s \in S} \frac{1}{|\mathcal{C}_s|}.$$

Since $\sum_{s \in S} \frac{1}{|\mathcal{C}_s|}$ equals the number of orbits, the desired formula follows.

■

Problem 3. *How many necklaces can be designed with 17 pearls black and white if pearls with the same color are indistinguishable.*

Solution: Denote by S the set of all the necklaces of 17 pearls (having a lock) that can be designed with black and white pearls. Since $|S| = 2^{17}$, the dihedral group $G = D_{34}$ acts on S in the obvious way. Since we are interested in the necklaces having no lock, for us two necklaces are the same if and only if they are in the same orbit with respect to the action of G on S. So we only need to count the number of orbits given by this action. The identity of G fixes the 2^{17} necklaces; each of the 16 nontrivial rotations fixes 2 necklaces (this is because 17 is prime); and each of the 17 inversions fixes 2^9 necklaces. Therefore, by the formula for counting orbits given in the previous problem, the number of necklaces we can design is

$$\frac{1}{34}(2^{17} + 16 * 2 + 17 * 2^9) = 2^8 + \frac{2^{16} + 16}{17}.$$

Note that, by Fermat's little theorem, 17 divides $2^{16} + 2^4 = (2^{16} - 1) + 17$.

■

Problem 4. *Classify the groups of order* 20*.*

Solution: Let G be a group of order 20. If G is abelian, then it follows by the fundamental theorem of finitely generated abelian groups that G is isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ or $\mathbb{Z}_4 \times \mathbb{Z}_5$.

Let G be a non-abelian group of order 20. Let n_5 be the number of 5-Sylow subgroups of G. By Sylow's theorems, $n_5 = 1$. Since there exists only one subgroup N of G having order 5, N must be normal. Let H be a 2-Sylow subgroup. Then G is the semidirect product of N and H, namely $G \cong N \rtimes_\phi H$ where $\phi\colon H \to \mathrm{Aut}(N)$.

Suppose first that H is isomorphic to the cyclic group $\mathbb{Z}_4$. If ϕ is a nontrivial homomorphisms, it maps the generator of $\mathbb{Z}_4$ to the unique element of order 2 of $\mathbb{Z}_4$ or to one of the two elements of order 4. Mapping the generator for each of the elements of order 4 gives isomorphic non-abelian groups. Let ϕ_1 and ϕ_2 be the homomorphisms we obtain when the generator of $\mathbb{Z}_4$ is mapped to an element of order 2 or an element of order 4, respectively. Since $|\ker \phi_1| = 2$ and $|\ker \phi_2| = 1$, the groups $\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4$ and $\mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$ are not isomorphic.

Suppose now that H is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. There are three nontrivial homomorphisms $\phi\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$; they are given by sending two nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ to the unique element of order two in $\mathbb{Z}_4$, and the other two elements to the identity. By the symmetry of the Klein group, the semidirect products induced by those ϕ are isomorphic non-abelian groups. Then $G \cong \mathbb{Z}_5 \rtimes_{\phi_3} (\mathbb{Z}_2 \times \mathbb{Z}_2)$ where ϕ_3 is one of the two homomorphisms just mentioned. The group found in this paragraph is not isomorphic to any of the groups found in the previous paragraph since $\mathbb{Z}_5 \rtimes_{\phi_0} \mathbb{Z}_2 \times \mathbb{Z}_2$ does not have any element of order 4. The absence of elements of order 4 forces $\mathbb{Z}_5 \rtimes_{\phi_3} \mathbb{Z}_2 \times \mathbb{Z}_2$ to be isomorphic to D_{20}.

■

Problem 5. *Show that the following groups are infinite and non-abelian.*

1. $G = \langle x, y \mid xyx = y \rangle$.
2. $G = \langle x, y \mid x^2 = y^2 = e \rangle$.

Solution: First, let us consider $G = \langle x, y \mid xyx = y \rangle$. Let $F = F(x, y)$ denote the free group on the set of two elements $\{x, y\}$, and let $GL_2(\mathbb{F}_2)$ be the general linear group over the field of two elements. Define $\phi\colon F \to M_2(\mathbb{F})$ by

$$\phi(x) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \phi(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By definition, $G = F/N$, where N is the minimal normal subgroup of F containing $xyxy^{-1}$. Since

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

it follows that $N \subseteq \ker \phi$ and, therefore, there exists a group homomorphism $\bar{\phi} \colon G \to GL_2(\mathbb{F}_2)$ such that $\bar{\phi}(G) = \phi(F)$. Notice that the image of G through $\bar{\phi}$ do not commute. Then G is not commutative. To see that G is infinite we proceed similarly. We define the map $\tau \colon F \to \mathbb{Z}_2 \oplus \mathbb{Z}$ by $\tau(x) = (1, 0)$ and $\tau(y) = (0, 1)$ and observe that $N \subseteq \ker \tau$. Therefore the subgroup H of $\mathbb{Z}_2 \oplus \mathbb{Z}$ generated by $(1, 0)$ and $0, 1$ is the homomorphic image of G. Since H is infinite, so is G.

Now let us consider $G = \langle x, y \mid x^2 = y^2 = e \rangle$. Let F be the free group on $\{x, y\}$, and let N be the minimal normal subgroup of G containing both x^2 and y^2. Let $S_{\mathbb{N}}$ be the symmetric group on $\mathbb{N} = \{1, 2, 3, \dots\}$, and define a group homomorphism $\sigma \colon F \to S_{\mathbb{N}}$ by

$$\sigma(x) = (1, 2)(3, 4)(4, 5) \cdots \quad \text{and} \quad \sigma(y) = (1)(2, 3)(4, 5)(5, 6) \cdots .$$

As the subgroup H of $S_{\mathbb{N}}$ generated by $\sigma(x)$ and $\sigma(y)$ is the homomorphic image of G, it suffices to verify that H is infinite and non-abelian. As $(\sigma(x) \circ \sigma(y))(1) = 2$ and $(\sigma(y) \circ \sigma(x))(1) = 3$, the subgroup H is not abelian. Finally, $(\sigma(y) \circ \sigma(x))(2k - 1) = 2k + 1$ for each $k \in \mathbb{N}$, it follows that $\sigma(y) \circ \sigma(x)$ is an element of H of infinite order. Hence H must be infinite. ■

Problem 6. *(I.52)*
(a) Show that push-outs (i.e., fiber coproducts) exist in the category of abelian groups. In this case the fiber coproduct of two homomorphisms f, g is denoted by $X \oplus_Z Y$. Show that it is the factor group

$$X \oplus_Z Y = (X \oplus Y)/W,$$

where W is the subgroup consisting of all elements $(f(z), -g(z))$ with $z \in Z$.
(b) Show that the push-out of an injective homomorphism is injective.

Solution: Let $f \colon Z \to X$ and $g \colon Z \to Y$ be group homomorphisms. Since X and Y are abelian groups, so is $X \oplus_Z Y$. Define $h \colon Z \to X \oplus_Z Y$ by $h(z) = (f(z), -g(z)) + W$. Also, define $i_1 \colon X \to X \oplus_Z Y$ by $i_1(x) = (x, 0) + W$ and $i_2 \colon Y \to X \oplus_Z Y$ by $i_2(y) = (0, y) + W$. The fact that i_1 and i_2 are homomorphisms follows immediately. We will show that $(X \oplus_Z Y, i_1, i_2)$ is a fiber coproduct in the category of abelian groups. Take an abelian group A along with homomorphisms $\phi_1 \colon X \to A$ and $\phi_2 \colon Y \to A$. Suppose that $h' \colon Z \to A$ is a homomorphism such that the following diagram commutes (without taking into account the doted lines).

$$\begin{tikzcd}
A & & \\
& X \oplus_Z Y \arrow[ul, dotted, "\phi"'] & Y \arrow[l, "i_2"'] \arrow[ull, bend right, "\phi_2"'] \\
& X \arrow[u, "i_1"] \arrow[uul, bend left, "\phi_1"] & Z \arrow[l, "f"] \arrow[u, "g"']
\end{tikzcd}$$

Define $\phi \colon X \oplus_Z Y \to A$ by $\phi((x, y) + W) = \phi_1(x) + \phi_2(y)$. If $(x_1, y_1) + W = (x_2, y_2) + W$, there exists $z \in Z$ such that $f(z) = x_2 - x_1$ and $-g(z) = y_2 - y_1$. So

$$\phi_1(x_2 - x_1) = \phi_1(f(z)) = \phi_2(g(z)) = -\phi_2(y_2 - y_1),$$

which implies that $\phi_1(x_1) + \phi_2(y_1) = \phi_1(x_2) + \phi_2(y_2)$. Then ϕ is a well-defined map. We represented ϕ using doted point in the above diagram. Since ϕ_1 and ϕ_2 are group homomorphisms, so is ϕ. We check now that the above diagram commutes. Since for $x \in X$, $\phi(i_1(x)) = \phi(x, 0) = \phi_1(x)$, the bottom left triangle commutes. In the same way, it can be seen that the bottom right triangle commutes. For $z \in Z$, $\phi(h(z)) = \phi(i_1(f(z))) = \phi_1(f(z))$. Therefore the big left vertical triangle commutes. In a similar way, it can be checked that the big right vertical triangle commutes. Substituting h' by $\phi_1 \circ f$, we can see that the same images are obtained by going down the diagram either via h' or via ϕ. Hence the above diagram commutes.

To check uniqueness of ϕ, suppose that $\psi \colon X \oplus_Z Y \to A$ also makes the above diagram commutes. Then for $x \in X$ and $y \in Y$,

$$\begin{aligned} \psi((x,y)+W) &= \psi(i_1(x)+i_2(y)) \\ &= \psi(i_1(x)) + \psi(i_2(y)) \\ &= \phi_1(x) + \phi_2(y) \\ &= \phi((x,y)+W). \end{aligned}$$

(b) If $i_1(y) \in W$ for some $y \in Y$, there exists $z \in Z$ such that $f(z) = 0$ and $-g(z) = y$. Since f is injective, $z = 0$, and so $y = -g(0) = 0$. Therefore the push-out i_2 of f is also injective.

■

Problem 7. *(Lang III.16) Prove that the inverse limit of a system of simple groups in which the homomorphisms are surjective is either the trivial group or a simple group.*

Solution: Let (G_i, f_i^j) be a system of simple groups where for each pair $j \geq i$ the homomorphism f_i^j is surjective. Since each G_i is simple, each f_i^j is either trivial or an isomorphism. Suppose that G_i and G_j are nontrivial. Take k such that $k \geq i$ and $k \geq j$. Since f_i^k and f_j^k are isomorphisms, $G_i \cong G_k \cong G_j$. Hence all nontrivial groups in the system are isomorphic. Let (G, f_i) be the inverse limit of (G_i, f_i^j). Since G is a subgroup of $\prod G_j$ and $f_i \cong G \to G_i$ is the restriction of the projection $\pi_i \cong \prod G_j \to G_i$ to G, if G_i is trivial for all i then G is also trivial. So assume that there exists i such that G_i is nontrivial. In this the case, we will show that $G \cong G_i$. There is no loss in assuming that G_j is nontrivial for all j (i.e. $G_j \cong G_i$ for all j). We show that f_i is an isomorphism.

First let us check that f_i is surjective. Take $g_i \in G_i$. For any index j there exists k such that $k \geq j$ and $k \geq i$. Then we take $g_j = f_j^k(g_k)$ where g_k is the unique element in G_k such that $f_i^k(g_k) = g_i$. If k' also satisfies that $k' \geq j$ and $k' \geq i$, take m such that $m \geq k$ and $m \geq k'$. Since $f_i^k(g_k) = g_i = f_i^{k'}(g_{k'})$, g_k and $g_{k'}$ must lift to the same element $g_m \in G_m$. Therefore $f_j^k(g_k) = f_j^m(g_m) = f_j^{k'}(g_{k'})$, which implies that g_j does not depend on the k chosen. It follows immediately that for $p \geq q$, $f_q^p(g_p) = g_q$. So (g_j) is actually an element in G satisfying that $f_i((g_j)) = g_i$. Hence f_i is surjective.

Now we show that f_i is injective. Suppose that (g_j) is in the kernel of f_i. Then $g_i = 1$. For any j there exists k such that $k \geq i$ and $k \geq j$. Since $f_i^k(g_k) = g_i = 1$, $g_k = 1$. Therefore $g_j = f_j^k(g_k) = 1$. Then (g_j) is the identity of G, which proves that f_i is injective. Hence $G \cong G_i$ is simple.

■

2 Ring Theory

Problem 8. *(Lang IV.5) Analyze irreducibility in the following cases:*
(a) $x^6 + x^3 + 1$ *over the rational numbers.*
(b) $x^2 + y^2 - 1$ *over the complex numbers.*
(c) $x^4 + 2011x^3 + 2012x^2 + 2013$ *over the rational numbers.*

Solution: (a) Let $p(x) = x^6 + x^3 + 1$. Note that the polynomial $p(x)$ is irreducible if and only if so is $q(x) = p(x+1)$. The polynomial $q(x) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$

has all its non-leading coefficients in the prime ideal (3). Since the constant coefficient of $q(x)$ is not in the ideal (9), by Eisenstein Criterion, $q(x)$ is irreducible over $\mathbb{Z}$. By Gauss's Lemma, $q(x)$ is also irreducible in $\mathbb{Q}$. Therefore the polynomial $x^6 + x^3 + 1$ is irreducible over the rationals.

(b) Consider the polynomial $q(x, y) = x^2 + y^2 - 1 = y^2 + (x^2 - 1)$ as a polynomial in the variable y with coefficients in $\mathbb{C}[x]$. The polynomial $q(x, y)$ is monic with non-leading coefficients in the prime ideal $(x-1)$ of $\mathbb{C}[x]$. Since the constant coefficient x^2-1 is not an element of $((x-1)^2)$, by Eisenstein Criterion, $q(x, y)$ is irreducible in $\mathbb{C}[x][y]$ as a polynomial in the variable y with coefficients in $\mathbb{C}[x]$. Hence $q(x, y)$ is irreducible as a polynomial in two variables.

(c) Let $r(x) = x^4 + 2011x^3 + 2012x^2 + 2013$. It is enough to check, by Gauss's lemma, that $r(x)$ is irreducible over $\mathbb{Z}$. Also, note that if $r(x)$ reduces over $\mathbb{Z}$ then $\bar{r}(x)$ reduces over $\mathbb{Z}_2$, where $\bar{r}(x) \in \mathbb{Z}_2[x]$ is the result of reducing the coefficients of $r(x)$ module 2. Since $\bar{r}(x) = x^4 + x^3 + 1$. Since $\bar{r}(x)$ does not have any roots in $\mathbb{Z}_2$, should it factor in $\mathbb{Z}_2[x]$, it would be the product of two irreducible polynomials of degree 2. However, there is only one irreducible polynomial of degree two in $\mathbb{Z}_2[x]$, namely $x^2 + x + 1$. Since $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq \bar{r}(x)$, $\bar{r}(x)$ must be irreducible over $\mathbb{Z}_2$. Hence, $r(x)$ is irreducible over the rationals.

■

Problem 9. *(Lang II.6) Let A be a factorial ring and p be a prime element. Show that the local ring $A_{(p)}$ is principal.*

Solution: Let $\mathcal{I}$ be a proper ideal of $A_{(p)}$, and let $\mathcal{M} = \{\frac{a}{b} \colon a \in (p) \text{ and } b \notin (p)\}$ be the only maximal ideal of $A_{(p)}$. Since $A_{(p)}$ is a commutative ring with 1, any ideal is contained in a maximal ideal; in particular, $\mathcal{I} \subset \mathcal{M}$. Since $\mathcal{M} = \langle \frac{p}{1} \rangle$, any element of $\mathcal{I}$ can be written as $\frac{mp^k}{b}$ where $m \notin (p)$ and $b \notin (p)$ (note that $\frac{m}{b}$ is a unit). Let n_0 be the minimal positive integer such that $\frac{p^{n_0}}{1} \in \mathcal{I}$. We shall show that $\mathcal{I} = \langle \frac{p^{n_0}}{1} \rangle$. Since $\mathcal{I}$ is an ideal, $\langle \frac{p^{n_0}}{1} \rangle \subset \mathcal{I}$. To show that reverse containment, take $\frac{mp^k}{b} \in \mathcal{I}$. By the minimality of n_0, $k \geq n_0$ and, therefore,

$$\frac{mp^k}{b} = \frac{mp^{k-n_0}}{b} \cdot \frac{p^{n_0}}{1} \in \langle \frac{p^{n_0}}{1} \rangle.$$

Hence every ideal of $A_{(p)}$ is principal.

■

Problem 10. *Let $\mathbb{F}$ be a field. Show that $\mathbb{F}[[x]]$ is factorial.*

Solution: Let $R = \mathbb{F}[[x]]$. We will prove that R is a principal ideal domain, which is, in fact, a stronger statement. Let $a = \sum a_n x^n$ be an element of R. There exists $b = \sum b_n x^n$ such that $ab = ba = 1$ if and only if $a_0 \neq 0$. To see this we take $b_0 = a_0^{-1}$, and once we have chosen $b_0, \dots, b_{n-1}$ in $\mathbb{F}$, we take $b_n \in \mathbb{F}$ such that $a_0 b_n + \cdots + a_n b_0 = 0$. Therefore $a_0 \neq 0$ implies that a is a unit. Hence $\mathcal{M} = (x)$ is the only maximal ideal of R. Since R is a commutative ring with 1, every ideal must be contained in a maximal ideal. This implies that each nonzero ideal of R is of the form (x^i) for some $i \geq 0$. Hence R is a principal ring (PID) and, therefore, a factorial ring (UFD).

■

Problem 11. *Let F be a field. Show that the ring of Laurent polynomials is principal.*

Solution: Let $R = F[x, 1/x]$ be the ring of Laurent polynomials over F. For $f(x) = \sum_{i=-k}^{n} a_i x^i \in R$ with $a_{-k} \neq 0$, we define $\operatorname{indeg}(f)$ to be k if $k > 0$ and zero otherwise. Now suppose that $\bar{I}$ is an ideal of R. Consider the ideal I generated by the set $S = \{x^{\operatorname{indeg}(r)} r(x) \mid r(x) \in \bar{I}\}$. Since I is an ideal of $F[x]$, which is a principal ring (PID), $I = (g(x))$. We show that $\bar{I} = (g(x))$ where $((g(x))$ is considered an ideal of R. Take an arbitrary element $a(x) \in \bar{I}$. Then we have that $x^{\text{indeg}(a)}a(x) \in I$, and so there exists $b(x) \in R$ such that $a(x) = x^{-\text{indeg}(a)}b(x)g(x) \in (g(x))$. On the other hand, every element of S belongs to $\bar{I}$; this is because $\bar{I}$ is an ideal. Therefore $(g(x)) = (S) \subset \bar{I}$. Hence $\bar{I} = (g(x))$ is principal, and this implies, in turn, that R is a principal ring.

■

Problem 12. *(Lang III.17) Let n range over the positive integers and let p be a prime number. Show that the abelian groups $A_n \approx \mathbb{Z}/p^n\mathbb{Z}$ form an inverse system under the canonical homomorphisms if $n \geq m$. Let Z_p be its inverse limit. Show that Z_p maps surjectively on each $\mathbb{Z}/p^n\mathbb{Z}$; that Z_p has no divisor of 0, and has a unique maximal ideal generated by p. Show that Z_p is factorial, with only one prime, namely p itself.*

<u>Solution:</u> The set of natural numbers is a special case of directed system of indices. If $n \geq m$ then $p^n\mathbb{Z} \subseteq p^m\mathbb{Z}$ and so $q^n_m \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ given by $a + p^n\mathbb{Z} \mapsto a + p^m\mathbb{Z}$ where $a \in \mathbb{Z}$ is a well-defined surjective homomorphism. Also if $n \geq m \geq k$,

$$(q^m_k \circ q^n_m)(a + p^n\mathbb{Z}) = q^m_k(a + p^m\mathbb{Z}) = a + p^k\mathbb{Z} = q^n_k(a + p^n\mathbb{Z}).$$

Hence (A_n, q^n_m) is an inverse system.

Denote by f_j the homomorphism from Z_p to A_j. Fix the index i and take $a_i \in A_i$. Define a_{i+j} such that $q^{i+j}_{i+j-1}(a_{i+j}) = a_{i+j-1}$ recursively starting at $j = 1$. Also define $a_j = q^i_j(a_i)$ for $i \geq j$. It follows that $q^t_s(a_t) = a_s$ for any $t \geq s$, which implies that $(a_j) \in Z_p$. Since $f_i((a_j)) = a_i$, f_i is surjective.

To check that A_p does not contain any zero divisors, take $(a_j + p^j\mathbb{Z})$ and $(b_j + p^j\mathbb{Z})$ in Z_p whose product is zero. Suppose, by way of contradiction, that there exist r and s such that p^r does not divide a_r and p^s does not divide b_s. Therefore neither p^r divides a_{r+s} nor p^s divides b_{r+s}. Then p^{r+s} does not divide $a_{r+s}b_{r+s}$, which means that $a_{r+s}b_{r+s} + p^{r+s}\mathbb{Z}$ is nonzero. But this contradicts that the product of $(a_j + p^j\mathbb{Z})$ and $(b_j + p^j\mathbb{Z})$ is zero. Hence either $(a_j + p^j\mathbb{Z})$ or $(b_j + p^j\mathbb{Z})$ must be zero. Therefore Z_p has no zero divisors.

To prove that the ideal $\mathcal{M}$ generated by p is the unique maximal ideal of Z_p, take an element $(a_j + p^j\mathbb{Z})$ in Z_p which is not in $\mathcal{M}$. Then p does not divide a_j, which implies that $(a_j, p^j) = 1$. Take, for each j, b_j such that $a_jb_j = 1$ in $\mathbb{Z}/p^j\mathbb{Z}$. Since p^j divides both $a_{j+1}b_{j+1} - 1$ and $a_jb_j - 1$, and $a_{j+1} \equiv a_j \pmod{p^j}$, we have that p^j divides $a_j(b_{j+1} - b_j)$. Therefore p^j divides $b_{j+1} - b_j$, which implies that $q^{j+1}_j(b_{j+1} + p^{j+1}\mathbb{Z}) = b_j + p^j\mathbb{Z}$. Hence $(b_j + p^j\mathbb{Z})$ is the inverse of $(a_j + p^j\mathbb{Z})$ in Z_p. Since any element outside $\mathcal{M}$ is a unit, $\mathcal{M}$ is the unique maximal ideal of Z_p. Thus Z_p is a local ring.

Since Z_p is a commutative ring with identity, any ideal is contained in a maximal ideal. On the other hand, $\mathcal{M}$ is the unique maximal ideal of Z_p, so any ideal is contained in $\mathcal{M}$. This implies that every ideal of Z_p is principal. Hence Z_p is a principal ring (PID). In particular, Z_p is a factorial ring (UFD). Since $\mathcal{M}$ is a prime ideal, p is prime in Z_p. Suppose that q is a prime. Then the ideal (q) is contained in $\mathcal{M}$. Hence $q = up^k$ where u is a unit. Since q is irreducible, $k = 1$, which implies that q is associate with p. Hence p is the unique prime in Z_p.

■

Problem 13. *Let ω be a root of $x^2 - x + 1$. Show that $\mathbb{Z}[\omega]$ is an Euclidean domain.*

<u>Solution:</u> Let $R = \mathbb{Z}[\omega]$. Since $x^6 - 1 = (x^3 - 1)(x + 1)(x^2 - x + 1)$, we have that ω is a sixth root of unity; in fact, a primitive sixth root of unity. We can assume, without loss of generality, that ω is the principal sixth root of unity. Therefore, R consists of all intersections of the following lines:
(i) lines parallel to the real axis intersecting the imaginary axis at $ib\frac{\sqrt{3}}{2}$ where $b \in \mathbb{Z}$;
(ii) lines whose slopes equal $\sqrt{3}$ intersecting the imaginary axis at $ib\sqrt{3}$ where $b \in \mathbb{Z}$;

(ii) lines whose slopes equal $-\sqrt{3}$ intersecting the imaginary axis at $ib\sqrt{3}$ where $b \in \mathbb{Z}$.
Therefore the points of R form a grid in $\mathbb{C}$ consisting of unit-side equilateral triangles. This implies that for any $z \in \mathbb{C}$ there exists $p \in R$ such that $|z - p| \le \frac{\sqrt{3}}{3}$. Therefore, for $a, b \in R$ such that $b \neq 0$, there exists $q \in R$ such that $|a/b - q| \le \frac{\sqrt{3}}{3}$. Taking $r = a - qb$, we have that

$$|r| = |a - qb| = |a/b - q||b| \le \frac{\sqrt{3}}{3}|b| < |b|.$$

Therefore $a = qb + r$ where $|r| < |b|$. Hence R is an Euclidean domain.

■

Problem 14. *Let R be a semisimple ring, $L \subset R$ be a left ideal. Prove that $L = Re$ for some idempotent e.*

Solution: Consider L as a left R-submodule of R. Since R is semisimple as a module over itself, there exists a left R-submodule L' of R such that $R = L \oplus L'$. Take $e \in L$ and $e' \in L'$ such that $1 = e + e'$. Then we have that

$$e + 0 = e = e(e + e') = e^2 + ee'.$$

Since R is the direct sum of L and L', it follows that $e = e^2$ and $0 = ee'$. So e is an idempotent element in R. Since L is a left R-submodule and $e \in L$, we have that $Re \subset L$. Now if $l \in L$,

$$l + 0 = l = l(e + e') = le + le'.$$

Consequently $l = le$ and $0 = le'$. Since $l = le \in Re$, we conclude that $L = Re$.

■

Problem 15. *Determine up to isomorphism all semisimple rings of order* 1008. *How many of them are commutative?*

Solution: Let R be a semisimple ring of order $1008 = 2^4 * 3^2 * 7$. Since R is finite, it is Artinian. Therefore, by Artin-Wedderburn theorem, R is the product of finitely many $n_i \times n_i$ matrix rings over division rings R_i. Since R is finite, so is R_i for each index i. So each R_i must be a field. The possible products of matrix rings with entries in a field of characteristic 2 are $M_2(\mathbb{F}_2)$, $\mathbb{F}_{16}$, $\mathbb{F}_4 \times \mathbb{F}_4$, $\mathbb{F}_4 \times \mathbb{F}_2 \times \mathbb{F}_2$, and $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Using fields of characteristic 3, instead of characteristic 2, the possible products of matrix rings are $\mathbb{F}_9$ and $\mathbb{F}_3 \times \mathbb{F}_3$. In characteristic 7 there is only one of such products, namely $\mathbb{F}_7$. Combining the products we have obtained before, we obtain a representative for each isomorphism class of semisimple rings of order 1008. There are 10 isomorphism classes. Only the representatives containing as a factor an $n \times n$ matrix ring where $n > 1$ are not commutative. Hence, up to isomorphism, there are eight commutative semisimple rings of order 1008.

■

3 Module Theory

Problem 16. *Let P be a cyclic projective module over an arbitrary ring R. Prove that $P \cong Re$ for some idempotent e of R.*

Solution: Since P is cyclic, there exists $x \in P$ such that $P = Rx$. Define $g_x \colon R \to Rx$ by $g_x(r) = rx$. It is easy to check that g_x is an R-module homomorphism. Also notice that $\ker(g_x) = \mathrm{Ann}(x)$. Therefore, we have the following short exact sequence

$$0 \to \mathrm{Ann}(x) \xrightarrow{i} R \xrightarrow{g_x} R_x \to 0.$$

Since Rx is projective, there exists a homomorphism $f\colon Rx \to R$ such that $g_x \circ f = \mathbb{1}_{Rx}$. This implies that $f(x)x = x$. Define $e \in R$ to be $f(x)$, and observe that $(e-1)x = 0$. So $e - 1 = \operatorname{Ann}(x)$. For $a \in \operatorname{Ann}(x)$ such that $1 = e + a$, we have

$$e = (e+a)e = e^2 + ae = e^2 + af(x) = e^2 + f(ax) = e^2 + f(0) = e^2.$$

Hence e is an idempotent element. Since $g_x \circ f = \mathbb{1}_{Rx}$, the map f is injective. Therefore $Re \cong Rx$, being Re the image of Rx by f.

■

Problem 17. *(Lang III.10) (a) Let A be a commutative ring with identity. If $\mathfrak{p}$ is a prime ideal, and $S = A - \mathfrak{p}$ is the complement of $\mathfrak{p}$ in the ring A, then $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$. Show that the natural map*

$$M \to \prod M_{\mathfrak{p}}$$

of a module M into the direct product of all localizations $M_{\mathfrak{p}}$ where $\mathfrak{p}$ ranges over all maximal ideals, is injective.
(b) Show that the sequence $0 \to M' \to M \to M'' \to 0$ is exact if and only if the sequence $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$ is exact for all prime $\mathfrak{p}$.
(c) Let A be an entire ring and let M be a torsion-free A-module. For each prime $\mathfrak{p}$ of A show that the natural map $M \to M_{\mathfrak{p}}$ is injective, but you can see that directly from the embedding of A in its quotient field K.

Solution: (a) Let $\mathcal{A}$ be the annihilator of M. Since A is a commutative ring with identity, $\mathcal{A}$ is a nontrivial proper ideal of A. Also, there exists a maximal ideal $\mathcal{M}$ containing $\mathcal{A}$. Denote $M \to \prod M_{\mathfrak{p}}$ by ϕ. If $m \in \ker(\phi)$, the projection of m in the factor corresponding to $\mathfrak{p} = \mathcal{M}$ is trivial, which means that $\frac{m}{1} = \frac{0}{s}$ for some $s \notin \mathcal{M}$. Therefore $sm = 0$. Since $s \notin \mathcal{A}$, we have $m = 0$. Hence ϕ is injective.

(b) If the sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact, for all prime ideal $\mathfrak{p}$, the sequence

$$0 \to M'_{\mathfrak{p}} \xrightarrow{\bar{f}} M_{\mathfrak{p}} \xrightarrow{\bar{g}} M''_{\mathfrak{p}} \to 0$$

is also exact. Conversely, suppose that the sequence (1) is exact for all prime ideals $\mathfrak{p}$ of A. We will show that the sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is also exact. Suppose that $f(m') = 0$ for some $m' \in M'$. Then $\bar{f}(\frac{m'}{1}) = \frac{f(m')}{1} = \frac{0}{s_{\mathfrak{p}}}$ in $M_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$. Since $\bar{f}$ is injective, $\frac{m'}{1} = 0$ in each $M_{\mathfrak{p}}$. By part (a), $m' = 0$. Therefore f is injective. Now we show that g is surjective. Suppose, on the contrary, that there exists $m'' \in M'' - g(M)$. Note that $\mathcal{A} := \operatorname{Ann}(m'' + g(M))$ in $M''/g(M)$ is not trivial. Let $\mathcal{M}$ be a maximal ideal containing $\mathcal{A}$. Since $\bar{g}$ is surjective, there exists $\frac{m}{s} \in M_{\mathcal{M}}$ such that $\bar{g}(\frac{m}{s}) = \frac{g(m)}{s} = \frac{m''}{1}$. So $sm'' = g(m) \in g(M)$, which means that $s \in \mathcal{A}$. But this contradicts that $s \in \mathcal{M}$. Hence g is surjective. Finally, we show that $\operatorname{Im}(f) = \ker(g)$. Take $m \in \operatorname{Im}(f)$ and $m' \in M'$ such that $f(m') = m$. It follows that

$$\frac{m}{1} = \frac{f(m')}{1} = \bar{f}\Big(\frac{m'}{1}\Big) \in \operatorname{Im}(\bar{f}) = \ker(\bar{g}).$$

Therefore $\frac{g(m)}{1} = \frac{0}{s}$ in $M''_{\mathfrak{p}}$ for some $s \in A - \mathfrak{p}$ for every prime ideal $\mathfrak{p}$. The injectivity of ϕ in part (a) implies that $g(m) = 0$ and so $\operatorname{Im}(f) \subseteq \ker(g)$. Take now $m \in \ker(g)$ and suppose, by way of contradiction, that $m \notin \operatorname{Im}(f)$. Then $m \in M - f(M')$. Since $1m \notin f(M')$, $\mathcal{A} := \operatorname{Ann}(m + f(M'))$ is a proper ideal of A. Let $\mathcal{M}$ be a maximal ideal containing $\mathcal{A}$. Since $\frac{m}{1} \in \ker(\bar{g}) = \operatorname{Im}(\bar{f})$, there exists $\frac{m'}{s} \in M'_{\mathcal{M}}$ such that $\bar{f}(\frac{m'}{s}) = \frac{f(m')}{s} = \frac{m}{1}$. Because $sm = f(m') \in f(M')$, $s \in \mathcal{A}$. But this is a contradiction because $s \in \mathcal{M}$. Therefore $\operatorname{Im}(f) \subseteq \ker(g)$, giving the desired result.

(c) Let $\psi\colon M \to M_{\mathfrak{p}}$ be the homomorphism given by $\psi(m) = \frac{m}{1}$. If $\psi(m) = 0$, we have that $\frac{m}{1} = \frac{0}{s}$ for some $s \in A - \mathfrak{p}$. Since $s \notin \mathfrak{p}$, we have that $s \neq 0$. The facts that M is torsion free and $s \neq 0$ imply that $m = 0$. Hence ψ is injective.

■

Problem 18. *Let R be a principal ring. Show that any projective R-module is free.*

Solution: Suppose that M is a projective module over R. Since M is projective, it is the direct summand of a free R-module, namely F. The R-module F is torsion-free because it is free. This implies that M is also torsion-free. Since R is a principal ring (PID), by the classification theorem of modules over PID, $M \cong R^I \oplus T$ where R^I is free and T is torsion. Since M is torsion-free, T is trivial. Hence M is free. ■

Problem 19. *Show that a finitely generated projective module over a local ring is free.*

Solution: Let R be a local ring and M be a finitely generated projective R-module. Take the smallest n such that $M = Rm_1 + \cdots + Rm_n$ for some $m_i \in M$. Since R^n is free, there exists an R-module homomorphism $\phi \cong R^m \to M$ inducing the following short exact sequence,

$$0 \to K \to R^m \xrightarrow{\phi} M \to 0,$$

where K is the kernel of ϕ. Since M is projective, the above sequence splits and then $M \oplus K \cong R^m$. Let $\mathcal{M}$ be the maximal ideal of R. Tensoring $M \oplus K \cong R^m$ with $R/\mathcal{M}$, we see that $(R/\mathcal{M})^n \cong M/\mathcal{M}M \oplus K/\mathcal{M}K$ as vector spaces over the field $R/\mathcal{M}$. The elements $\bar{m_1}, \dots, \bar{m_n}$ generate $M/\mathcal{M}M$ where $\bar{m_i} = m_i + \mathcal{M}M$. Suppose now that $\sum_i \bar{r}_i \bar{m_i} = 0$ for some $\bar{r}_i \in R/\mathcal{M}$. This implies that $\sum_i r_i m_i \in \mathcal{M}M$, and so that $r_i \in \mathcal{M}$ for all i. Therefore the elements $m_1, \dots, m_n$ are linearly independent in $M/\mathcal{M}M$, and so a basis. Hence $\dim M/\mathcal{M}M = n$, which implies that $N/\mathcal{M}N$ is trivial. Since $N = \mathcal{M}N$ and R is a local ring with maximal ideal $\mathcal{M}$, Nakayama's Lemma implies that $N = 0$. Therefore $M = R^n$ is a free R-module.

■

Problem 20. *(Lang III.19) Let (A_i, f_j^i) be a directed family of modules. Let $a_k \in A_k$ for some k, and suppose that the image of a_k in the direct limit A is 0. Show that there exists some index $m \geq k$ such that $f_m^k(a_k) = 0$. In other words, whether some element in some group A_i vanishes in the direct limit can already be seen within the original data.*

Solution: For the index i, let $f_i\colon A_i \to A$ be the map given by the direct limit. Let $S = \oplus_i A_i$ and, for $x_i \in A_i$, denote by $\bar{x}_i$ the element in the direct sum having x_i in the i-th component and zeros elsewhere. Let N be the subgroup of S generated by the elements $(\dots, 0, x, \dots, -f_j^i(x), 0, \dots)$ with $x \in A_i$ and $-f_j^i(x) \in A_j$ for $i \leq j$. The fact that $f_k(a_k) = 0$ implies that $\bar{a_k} \in N$. Then we can write $\bar{a_k}$ as

$$(\dots, 0, a_{i_1}, \dots, -f_{j_1}^{i_1}(a_{i_1}), 0, \dots) \dots (\dots, 0, a_{i_r}, \dots, -f_{j_r}^{i_r}(a_{i_r}), 0, \dots)$$

for some $r \geq 1$, where $i_t \leq j_t$ for $1 \leq t \leq r$. Although the indices i_t and j_t above can be spread over different components, the addition in the component s is zero when $s \neq k$ and a_k when $s = k$. Therefore, for $m \geq \max\{k, j_1, \dots, j_r\}$ (which must exist),

$$\begin{aligned} f_m^k(a_k) &= (f_m^{i_1}(a_{i_1}) - f_m^{j_1}(f_{j_1}^{i_1}(a_{i_1}))) + \cdots + (f_m^{i_r}(a_{i_r}) - f_m^{j_r}(f_{j_r}^{i_r}(a_{i_r}))) \\ &= (f_m^{i_1}(a_{i_1}) - f_m^{i_1}(a_{i_1})) + \cdots + (f_m^{i_r}(a_{i_r}) - f_m^{i_r}(a_{i_r})) \\ &= 0. \end{aligned}$$

Then m is the index we were looking for.

■

Problem 21. *(Lang III.24) Show that any module is a direct limit of finitely generated submodule.*

Solution: Let R be a ring and M be an R-module. For any finite subset S of M, denote by M_S the finite submodule of M generated by S. The finite subsets of M form a directed system of indices. For S and T finite subsets of M such that $S \subset T$, we denote by $i_{S,T}$ the inclusion from M_S to M_T. The family $(M_S, i_{S,T})$ is a directed system of finitely generated R-modules. We show that (M, i_S) where $i_S \colon M_S \to M$ is the inclusion is the direct limit of the family $(M_S, i_{S,T})$. For $S \subset T$, $i_T \circ i_{S,T} = i_S$. Consider (N, f_S) where N is an R-module and, for each finite subset S of M, $f_S \colon M_S \to N$ is an R-module such that $f_T \circ i_{S,T} = f_S$. Define $\phi \colon M \to N$ as follows. For $m \in M$, we set $\phi(m) = f_{\{m\}}(m)$. If S is a finite subset of M containing m, $f_S(m) = f_{\{m\}}(m)$. Therefore, if $a, b \in M$ and $\alpha \in R$, $\phi(\alpha a + b) = f_{\langle a,b \rangle}(\alpha a + b) = \alpha f_{\langle a \rangle} + f_{\langle b \rangle} = \alpha \phi(a) + \phi(b)$. Therefore ϕ is a homomorphism. Also for a finite subset S of M and $m \in M_S$, $\phi(i_S(m)) = \phi(m) = f_{\langle m \rangle}(m) = f_S(m)$. Hence M is the direct limit of its finitely generated submodules.

■

Problem 22. *(Lang III.21) Let (M_i', f_j^i), (M_i, g_j^i) be directed systems of modules over a ring. By a homomorphism*

$$(M_i') \xrightarrow{u} (M_i)$$

one means a family of homomorphisms $u_i \colon M_i' \to M_i$ for each i which commute with the f_j^i, g_j^i. Suppose we are given an exact sequence

$$0 \to (M_i') \xrightarrow{u} (M_i) \xrightarrow{v} (M_i'') \to 0$$

of directed systems, meaning that for each i, the sequence

$$0 \to M_i' \to M_i \to M_i'' \to 0$$

is exact. Show that the direct limit preserves exactness, that is

$$0 \to \varinjlim M_i' \to \varinjlim M_i \to \varinjlim M_i'' \to 0$$

is exact.

Solution: Denote by M', M, and M'' the direct limits $\varinjlim M_i'$, $\varinjlim M_i$, and $\varinjlim M_i''$ respectively, where (M_i'', h_j^i) is a directed system of modules with $v_i : M_i \to M_i''$ commuting with the g_j^i, h_j^i. It is enough to show that the sequence $M' \to M \to M''$ is exact at M since exactness at M' and M'' follows similarly by considering the sequences $0 \to M' \to M$ and $M \to M'' \to 0$.

We will show that $\ker(v) = \operatorname{Im}(u)$. For each $m' \in M'$, there exists i and $m_i' \in M_i'$ such that $m' = f_i(m_i')$. Considering the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_i' & \xrightarrow{u_i} & M_i & \xrightarrow{v_i} & M_i'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle g_i} & & \downarrow{\scriptstyle h_i} & & \\
0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0,
\end{array}$$

we obtain that

$$v(u(m')) = v(u(f_i(m_i'))) = v(g_i(u_i(m_i'))) = (v \circ g_i)(u_i(m_i')) = h_i(v_i(u_i(m_i'))) = h_i(0) = 0;$$

this is because $v_i \circ u_i$ is trivial. Therefore $\mathrm{Im}(u) \subseteq \ker(v)$. To show the reverse inclusion, take $m \in \ker(v)$. Then take i and $m_i \in M_i$ such that $m = g_i(m_i)$. Since $h_i(v_i(m_i)) = v(g_i(m_i)) = 0$, there exists $j \ge i$ such that $h^i_j(v_i(m_i)) = 0$. Hence $v_j(g^i_j(m_i)) = 0$. Since $g^i_j(m_i) \in \ker(v_j) = \mathrm{Im}(u_j)$, there exists $m'_j \in M'_j$ such that $u_j(m'_j) = g^i_j(m_i)$. Taking $m' = f_j(m'_j) \in M'$,

$$u(m') = u(f_j(m'_j)) = g_j(u_j(m'_j)) = g_j(g^i_j(m_i)) = g_i(m_i) = m.$$

Therefore $\ker(v) \subseteq \mathrm{Im}(u)$, which implies that the sequence $M' \to M \to M''$ is exact at M.

■

Problem 23. *(Lang III.23) Let (M_i) be a directed family of modules over a ring. For any module N show that*

$$\varprojlim \mathrm{Hom}(N, M_i) = \mathrm{Hom}(N, \varprojlim M_i).$$

<u>Solution:</u> For $i \le j$ denote by $f_{ji} \colon M_j \to M_i$ the homomorphisms in the directed family of modules (M_i), and denote by M its inverse limit. For $i \le j$ denote by $\bar{f}_{ji} \colon \mathrm{Hom}(N, M_j) \to \mathrm{Hom}(N, M_i)$ the homomorphism given by $\bar{f}_{ji}(\phi)(x) = f_{ji}(\phi(x))$ for $\phi \in \mathrm{Hom}(N, M_j)$ and $x \in N$. Since (M_i) is a directed family of modules, so is $(\mathrm{Hom}(N, M_i), \bar{f}_{ji})$. Denote by $\bar{f}_i$ the homomorphism from $\mathrm{Hom}(N, M)$ to $\mathrm{Hom}(N, M_i)$ given by $\bar{f}_i(\phi)(x) = f_i(\phi(x))$. We only need to show that $(\mathrm{Hom}(N, M), \bar{f}_i)$ is the inverse limit of the directed family of modules $(\mathrm{Hom}(N, M_i), \bar{f}_{ji})$.

If $\phi \in \mathrm{Hom}(N, M)$ and $x \in N$, we have that

$$(\bar{f}_{ji}(\bar{f}_j(\phi)))(x) = f_{ji}(\bar{f}_j(\phi)(x)) = f_{ji}(f_j(\phi(x))) = f_i(\phi(x)) = \bar{f}_i(\phi)(x),$$

for any $i \le j$. Therefore $\bar{f}_{ji} \circ \bar{f}_j = \bar{f}_i$ for $i \le j$ (i.e. the upper triangle in the diagram given below commutes). Now suppose that (A, α_i) where $\alpha_i \colon A \to \mathrm{Hom}(N, M_i)$ satisfies that $\bar{f}_{ji} \circ \alpha_j = \alpha_i$. Define $\alpha \colon A \to \mathrm{Hom}(N, M)$ by $\alpha(a)(x) = (\alpha_i(a)(x))$ for $a \in A$ and $x \in N$. If $i \le j$ $f_{ji}(\alpha_j(a)(x)) = \alpha_i(a)(x)$ for each $a \in A$ and $x \in N$. Therefore $(\alpha_i(a)(x)) \in M$ for each $a \in A$ and $x \in N$, which implies that $\alpha(a) \colon N \to M$ is a well-defined map. The map α is represented with dotted points in the following diagram,

$$\begin{tikzcd}
\mathrm{Hom}(N, M_j) \arrow[rr, "\bar{f}_{ji}"] & & \mathrm{Hom}(N, M_i) \\
& \mathrm{Hom}(N, M) \arrow[ul, "\bar{f}_j"'] \arrow[ur, "\bar{f}_i"] & \\
& A \arrow[uul, "\alpha_j"] \arrow[uur, "\alpha_i"'] \arrow[u, dotted, "\alpha"] &
\end{tikzcd}$$

For $a \in A$ the map $\alpha_i(a)$ is a homomorphism for each i, so the map $\alpha(a)$ is also a homomorphism. Then we have that α is well defined. The fact that α is a module homomorphism follows from the fact that α_i is a module homomorphism for each index i. Finally, for any index i and $a \in A$,

$$\bar{f}_i(\alpha(a))(x) = f_i(\alpha(a)(x)) = f_i((\alpha_j(a)(x))) = \alpha_i(a)(x),$$

for all $x \in N$. Therefore $\bar{f}_i \circ \alpha = \alpha_i$ for all index i (i.e. α respects the commutativity of the above diagram). Hence $(\mathrm{Hom}(N, M), \bar{f}_i)$ is the inverse limit of $(\mathrm{Hom}(N, M_i), \bar{f}_{ji})$.

■

4 Field Theory

Problem 24. *(Lang V.13) If the roots of a monic polynomial $f(x) \in k(x)$ in some splitting field are distinct, and form a field, then char$(k) = p$ and $f(x) = x^{p^m} - x$ for some $m \geq 1$.*

Solution: Let $F = \{r_1, \dots, r_n\}$ be the set of roots of f. Since F is a field, $k * 1$ is a root of f for any $k \in \mathbb{N}$. Since a polynomial has only finitely many roots, char$(k) = p$. Since f splits over F, namely $f(x) = (x - r_1) \dots (x - r_n)$, and F is trivially generated by the roots of f, F must be the splitting field of f. Let $\mathbb{F}_p$ be the prime field of F. Since F is a finite dimensional vector space over $\mathbb{F}_p$, $n = |F| = p^m$. We also know that the finite field of order p^m is the splitting field of the polynomial $x^{p^m} - x$. Therefore $f(x) = x^{p^m} - x$.

■

Problem 25. *(Lang V.14) Let char$(K) = p$. Let L be a finite extension of K, and suppose that $[L : K]$ prime to p. Show that L is separable over K.*

Solution: Take and element a in L. Since $[L : K]$ is finite, a is algebraic. Let $f(x) \in K[x]$ be the irreducible polynomial of a over K. Since $m = \deg f$ divides $n = [L : K]$, we have that $(m, p) = 1$. Let f_{sep} be a separable polynomial in $K[x]$ such that $f(x) = f_{sep}(x^{p^t})$ where t is a non-negative integer. This implies that $m = \deg f = p^t \deg f_{sep}$, and so p^t divides m. The fact that $(m, p) = 1$ forces t to be zero. Hence $f = f_{sep}$ is separable over K.

■

Problem 26. *(Lang V.15) Suppose that char$(K) = p$. Let $a \in K$. If a has no p-th roots in K, show that $x^{p^n} - a$ is irreducible in $K[x]$ for all positive integer n.*

Solution: Let n be a positive integer and $f(x) = x^{p^n} - a$. If β_1 and β_2 are roots of f in some splitting field, then we have that $(\beta_1 - \beta_2)^{p^n} = \beta_1^{p^n} - \beta_2^{p^n} = a - a = 0$, and so $\beta_1 = \beta_2$. Hence f is purely inseparable, and so there exists β in some splitting field F of f over K such that $f(x) = (x - \beta)^{p^n} = x^{p^n} - \beta^{p^n}$. If g is the irreducible polynomial of β over K, $g(x) = (x - \beta)^{p^k}$ in F for some k. The degree of g is a power of p because g is irreducible and purely inseparable. Since g divides f in $K[x]$ we have that $k \leq n$. If $k = n$ then $f(x) = g(x)$, and so f is irreducible. Assume, by way of contradiction, that $k < n$. Note that β^{p^k} is a coefficient of g, so $\beta^{p^k} \in K$. If $\alpha = \beta^{p^{n-1}}$ we have that $\alpha = (\beta^{p^k})^{p^{n-k-1}} \in K$. Then we have that $a = \alpha^p$ for some $\alpha \in K$. This contradicts the fact that a has no p-th roots in K.

■

Problem 27. *(Lang V.16) Let char$(K) = p$. Let α be algebraic over K. Show that α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integer n.*

Solution: First, let us assume that α is separable. Given that $K(\alpha^{p^n}) \subset K(\alpha)$, it is enough to prove that $\alpha \in K(\alpha^{p^n})$. Since α is a root of $f(x) = x^{p^n} - \alpha^{p^n} \in K(\alpha^{p^n})[x]$, the irreducible polynomial $g(x)$ of α over $K(\alpha^{p^n})$ divides $f(x)$. Therefore, $g(x) = (x - \alpha)^m$ in $K(\alpha^{p^n})[x]$. If $a(x)$ is the irreducible polynomial of α over K, then $g(x)$ divides $a(x)$ in $K(\alpha^{p^n})[x]$. Since $a(x)$ is separable, $m = 1$. Hence $\alpha \in K(\alpha^{p^n})$.

On the other hand, assume that $K(\alpha) = K(\alpha^{p^n})$ for all positive integer n. Let $a(x)$ be the irreducible polynomial of α over K. There exists a separable polynomial $a_{sep}(x) \in K[x]$ and a non-negative k such that $a(x) = a_{sep}(x^{p^k})$. Because α is a root of $a(x)$, the element α^{p^k} is a root of $a_{sep}(x)$. The fact that $a(x)$ is irreducible implies that $a_{sep}(x)$ is also irreducible. Therefore $a_{sep}(x)$ is the irreducible polynomial of α^{p^k}. It follows that

$$\deg a_{sep}(x) = [K(\alpha^{p^k}) : K] = [K(\alpha) : K] = \deg a(x).$$

This implies that $k = 0$, and so $a(x) = a_{sep}(x)$. Hence $a(x)$ is separable.

$\blacksquare$

Problem 28. *(Lang V.18) Show that every element of a finite field can be written as a sum of two squares in that field.*

Solution: Let F be a finite field. If $\text{char}(F) = 2$ then the Frobenius homomorphism is surjective, and so for any $y \in F$ there exists $x \in F$ such that $y = x^2 = x^2 + 0^2$. Suppose now that $\text{char}(F) = p$ is an odd prime. Then $|F|$ is odd, and so $|F^\times| = 2k$ for some natural k. In addition, $F^\times$ is cyclic; let $F^\times = \langle a \rangle$. Note that every even power of a is a square. Since 0 is also a square in F, at least $k+1$ elements of F are squares. Let S be the set of all squares in F. For an arbitrary element $y \in F$, the following inequality holds,

$$|y - S| = |S| = k + 1 \geq \frac{|F|}{2}.$$

By the Pigeonhole Principle, there exists $s \in (y - S) \cap S$, which means that $s = s_1^2$ for some $s_1 \in F$ and $s = y - s_2^2$ for some $s_2 \in F$. Hence $y = s_1^2 + s_2^2$.

$\blacksquare$

Problem 29. *(Lang V.24) Show that the primitive element theorem may not hold for a finite non-separable extension.*

Solution: Let $F = \mathbb{Z}_p(Y, Z)$ where Y and Z are two algebraically independent transcendental elements over $\mathbb{Z}_p$, and let F^a be an algebraic closure of F. Consider the polynomials $p(x) = x^p - Y$ and $q(x) = x^p - Z$ in $F[x]$. Since $p(x)$ and $q(x)$ are Eisenstein with respect to the prime ideals (Y) and (Z), both polynomials are irreducible in $\mathbb{Z}_p[Y, Z]$. By Gauss Lemma, they are also irreducible over F. Let α and β be respective roots of $p(x)$ and $q(x)$ in F^a. Consider the field extension $F(\alpha, \beta)/F$. Since $q(x) = (x - \beta)^p$ in F^a, if $q(x)$ reduced in $F(\alpha)$, we would have that $\beta^i \in F(\alpha)$ for some i, and so $\beta^i = \sum c_j \alpha^j$ for some $c_j \in F$. But this would imply that $Z^i = \sum c_j^p Y^j$, which cannot happen because Y and Z are algebraically independent. Therefore $q(x)$ is irreducible over $F(\alpha)$. This implies that

$$[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F] = p^2.$$

Now for $\gamma \in F(\alpha, \beta)$ there are $c_{ij} \in F$ such that $\gamma = \sum_{ij} c_{ij} \alpha^i \beta^j$. Thus

$$\gamma^p = \sum_{ij} c_{ij}^p (\alpha^i)^p (\beta^j)^p = \sum_{ij} c_{ij}^p Y^i Z^j \in F.$$

Hence $[F(\gamma) : F] \leq p$, which implies that $F(\alpha, \beta)$ cannot be a simple extension of F.

$\blacksquare$

Problem 30. *(Hungerford V.5.9) If $n \geq 3$, show that $x^{2^n} + x + 1$ is reducible over $\mathbb{F}_2$.*

Solution: Let $p(x) = x^{2^n} + x + 1$. Suppose, by way of contradiction, that $p(x)$ is irreducible. Let r be a root of $p(x)$ in some splitting field F. Then $[\mathbb{F}_2(r) : \mathbb{F}_2] = n$. This implies that $\mathbb{F}_2(r) = \mathbb{F}_{2^n}$. Also we know that $\mathbb{F}_{2^n}$ is the splitting field of the polynomial $q(x) = x^{2^n} - x \in \mathbb{F}_2[x]$. Notice that for any $a \in \mathbb{F}_{2^n}$

$$p(r + a) = (r + a)^{2^n} + (r + a) + 1 = (r^{2^n} + r + 1) + (a^{2^n} - a) = 0.$$

Therefore $r + a$ is a root of $p(x)$ for each $a \in \mathbb{F}_{2^n}$. Since $r + \mathbb{F}_{2^n} = \mathbb{F}_{2^n}$, any element in $\mathbb{F}_{2^n}$ is a root of $p(x)$. In particular, $0 = p(0) = 1$, which is a contradiction. Hence $p(x)$ is irreducible.

$\blacksquare$

Problem 31. *(Hungerford V.5.12) Let p be prime. Show that for any $n > 0$, there exists an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.*

Solution: We know that there exists, up to isomorphism, a unique field of order p^n. Denote this field by F. Let $F^\times$ be the multiplicative subgroup of units of F. Since F is a vector space over $\mathbb{F}_p$, and $|F| = p^n$, it follows that $[F : \mathbb{F}_p] = n$. Since $F^\times$ is finite, it must be cyclic. Therefore there exists $a \in F^\times$ such that $F^\times = \langle a \rangle$. Hence, $F = \mathbb{F}_p(a)$. Let $f(x)$ be the irreducible polynomial of a. Then $\deg f = [\mathbb{F}_p(a) : \mathbb{F}_p] = n$. Therefore $f(x)$ is an irreducible polynomial of degree n.

■

Problem 32. *(Hungerford V.3.24) Show that an algebraic extension E of F is is normal if and only if every irreducible $f \in F[x]$ factors in $E[x]$ as a product of irreducible polynomials all of them with the same degree.*

Solution: Suppose first that the extension E/F is normal. Let $f_1, \dots, f_k \in E[x]$ be non-constant irreducible polynomials such that $f = f_1 \dots f_k$. Let C be the set of coefficients of the polynomials $f_1, \dots, f_k$. By replacing E by the normal closure of $F(C)$ over F if necessary, we can assume that E/F is finite (because $F(C)/F$ is finite).

Now suppose that α and β are roots of f in some splitting field. and f_j, respectively. The problem follows trivially if $E = F$, so we assume that $E \neq F$. As E is normal over F neither α nor β are in E. As both α and β are roots of the same irreducible polynomial over F, say f, there exists an F-homomorphism $\sigma \colon F(\alpha) \to \bar{K}$ such that $\sigma(\alpha) = \beta$, where $\bar{K}$ is an algebraic closure of F containing E. Now the fact that $E(\alpha)/F(\alpha)$ is a finite extension allows us to extend the F-homomorphism σ to $\bar{\sigma} \colon E(\alpha) \to \bar{K}$. Since E is a normal extension of F it follows that $\bar{\sigma}(E) = E$ and, therefore, $\bar{\sigma}(E(\alpha)) = E(\beta)$. Hence $[E(\alpha) : F(\alpha)] = [E(\beta) : F(\beta)]$, which implies that

$$[E(\alpha) : E] = \frac{[E(\alpha) : F(\alpha)][F(\alpha) : F]}{[E : F]} = \frac{[E(\beta) : F(\beta)][F(\beta) : F]}{[E : F]} = [E(\beta) : E].$$

Now for any two index i and j, we can consider roots α_i and α_j of the irreducible polynomials $f_i, f_j \in E[x]$ (respectively) to obtain that $\deg f_i = [E(\alpha_i) : E] = [E(\alpha_j) : E] = \deg f_j$. This concludes the proof.

■

5 Galois Theory

Problem 33. *(Lang VI.11) A polynomial $f(x)$ is said to be reciprocal if whenever α is a root, then $1/\alpha$ is also a root. We suppose that f has coefficient in a real subfield k of the complex numbers. If f is irreducible over k, and has a non-real root of absolute value 1, show that f is reciprocal of even degree.*

Solution: Let β be a non-real root of $f(x)$ with absolute value 1, and let α be an arbitrary root of $f(x)$. Denote by K the splitting field of $f(x)$ inside $\mathbb{C}$, and denote by G the Galois group of the field extension K/k. Since $f(x)$ is irreducible over k, G acts transitively on the roots of $f(x)$. Then there exists $\sigma \in G$ such that $\sigma(\beta) = \alpha$. This implies that $\sigma(\bar{\beta}) = \sigma(1/\beta) = 1/\sigma(\beta) = \alpha^{-1}$. Since $\bar{\beta}$ is a root of $f(x)$ so is α^{-1}; this is because σ permutes the roots of $f(x)$. Hence $f(x)$ is reciprocal.

Since $f(x)$ is an irreducible polynomial over a field of characteristic zero, it is separable. We know that the non-real roots of $f(x)$ come in pairs. Since $f(x)$ is reciprocal, the real roots also come in pairs. Therefore $f(x)$ has an even number of roots in K. Hence the degree of $f(x)$ is even.

■

Problem 34. *(Lang VI.12) Find the Galois group of $x^5 - 4x + 2$ over the rationals.*

Solution: (a) Let $p(x) = x^5 - 4x + 2$ and G be the Galois group of $p(x)$. We think of G as a subgroup of S_5. By Eisenstein Criterion, the polynomial $p(x)$ is irreducible over $\mathbb{Z}$. Gauss Lemma then implies that $p(x)$ is irreducible over the rationals. Hence G contains a cycle of length 5. Since $p'(x) = 5x^4 - 4$ has only two real roots, $p(x)$ has at most three real roots. Given that $p(-\infty) = -\infty$, $p(0) = 2$, $p(1) = -1$, and $p(\infty) = \infty$, $p(x)$ has exactly three real roots. Since $p(x)$ has only two non-real roots, which are conjugates, the conjugation automorphism represent a transposition in G. Since $G \le S_5$ contains a 5-cycle and a transposition, $G = S_5$.

Problem 35. *(Lang VI 13) Find the Galois group of $x^4 + 2x^2 + x + 3$ over the rationals.*

Solution: Let $p(x) = x^4 + 2x^2 + x + 3$. Reducing mod 2, we have that $p(x) = x^4 + x + 1$. Since $p(x)$ does not have any roots in $\mathbb{Z}_2$, if it were irreducible it would have to factor as the product of two irreducible polynomials of degree 2 each. However, the only irreducible polynomial of degree 2 over $\mathbb{Z}_2$ is $X^2 + X + 1$, and $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq p(x)$. Therefore $p(x)$ is irreducible over $\mathbb{Z}_2$. Since every finite extension of a finite field is cyclic, the Galois group of $p(x)$ over $\mathbb{Z}_2$ contains an element of order 4. Therefore G contains an element of order 4.

Reducing now mod 3, we have that $p(x) = x(x^3 + 2x + 1)$. Since $x^3 + 2x + 1$ does not have any root in $\mathbb{Z}_3$, it is irreducible over $\mathbb{Z}_3$. Therefore the Galois group of $p(x)$ over $\mathbb{Z}_3$ contains an element of order 3. Then G contains an element of order 3.

Since G contains an element of order 3 and an element of order 4, $|G|$ is divisible by 12. The fact that G is isomorphic to a subgroup of S_4 implies that G is isomorphic to either A_4 or S_4. Since A_4 does not contain any element of order 4, G must be isomorphic to S_4.

■

Problem 36. *Find the Galois group of the polynomial $x^5 - 5$ over $\mathbb{Q}$.*

Solution: Let $p(x) = x^5 - 5$. By Eisenstein Criterion and Gauss Lemma, $p(x)$ is irreducible over $\mathbb{Q}$. Let $\alpha = \sqrt[5]{5}$ and ω be a primitive 5^{th}-root of unity. Then the splitting field of $p(x)$ over $\mathbb{Q}$ is $F = \mathbb{Q}(\alpha, \omega)$; this is because the roots of $p(x)$ are given by $\omega^i\alpha$ where $1 \le i \le 5$. Since α is a root of $p(x)$, which is irreducible over $\mathbb{Q}$, we have that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. On the other hand, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ since the irreducible polynomial of ω is the cyclotomic polynomial $x^4 + x^3 + x^2 + x + 1$. Since $(4, 5) = 1$, $[F : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] = 20$. Therefore the Galois group $G = Gal(F/\mathbb{Q})$ of $p(x)$ has order 20.

By Problem 1, S_5 does not contain any abelian subgroup of order 20. Hence G is not abelian. By Problem 4, G must be isomorphic to the dihedral of order 20 or to one of the two non-isomorphic semidirect products $\mathbb{Z}_5 \rtimes_\phi \mathbb{Z}_4$.

■

Problem 37. *(Lang VI.14) Prove that given a symmetric group S_n, there exists a polynomial $f(x) \in \mathbb{Z}[x]$ with leading coefficient 1 whose Galois group over $\mathbb{Q}$ is S_n.*

Solution: We saw previously that for any prime p and any $n \in \mathbb{N}$ there exists an irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ of degree n. Take an irreducible polynomial $p_2(x) \in \mathbb{F}_2[x]$ of degree n. Also take an irreducible polynomial $p_3(x) \in \mathbb{F}_3[x]$ of degree $n - 1$. Finally, take an irreducible polynomial $p_5(x) \in \mathbb{F}_5[x]$ of degree 2. By the Chinese remainder theorem, there exists a polynomial $f(x) \in \mathbb{Z}[x]$

such that

$$f(x) = p_2(x) \pmod 2 \tag{1}$$
$$f(x) = xp_3(x) \pmod 3 \tag{2}$$
$$f(x) = q(x)p_5(x) \pmod 5 \tag{3}$$

where $q(x)$ is the product of irreducible polynomials of odd degree chosen conveniently. Let G be the Galois group of $f(x)$ over the rationals seen as a subgroup of S_n. First equality implies that G contains an n-cycle; therefore, G is a transitive subgroup of S_n. The second and third equalities guarantees respectively the existence of an $(n-1)$-cycle and a transposition in G. As we have seen in previous problem, if a transitive subgroup of S_n contains an $(n-1)$-cycle and a transposition it has to be the full group. Hence, $G \cong S_n$.

■

Problem 38. *(Lang VI.23) Prove the following statements.*
(a) Let G be an abelian group. There exists an abelian extension of $\mathbb{Q}$ whose Galois group is G.
(b) Let k be a finite extension of $\mathbb{Q}$, and $G \neq \{1\}$ a finite abelian group. There exist infinitely many abelian extensions of k whose Galois group is G.

Solution: (a) By the fundamental theorem of finitely generated abelian groups, we have that $G \approx \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $n_1, \dots, n_k \in \mathbb{N}$. By Dirichlet theorem, for $i \in \{1, \dots, k\}$, there are infinitely many primes p, such that $p - 1 \in (n_i)$. Then we can take distinct primes $p_1, \dots, p_k$ such that $p_i - 1 \in (n_i)$. Since (p_i) and (p_j) are comaximal for $i \neq j$, if $n = p_1 \dots p_k$, by the Chinese remainder theorem, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$. This, in turn, implies that

$$(\mathbb{Z}_n)^\times \approx (\mathbb{Z}_{p_1})^\times \times \cdots \times (\mathbb{Z}_{p_k})^\times.$$

Therefore, we have that $(\mathbb{Z}_n)^\times \cong \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_k-1}$.

Now if ζ is a primitive n-th root of unity,

$$H = Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}_n)^\times \cong \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_k-1}.$$

Notice that H has a subgroup $N = N_1 \times \cdots \times N_k$ where N_i is a cyclic subgroup of $\mathbb{Z}_{p_i-1}$ of order $\frac{p_i-1}{n_i}$. Since N is abelian, N is a normal subgroup of H. Let F be the fixed field of N in the Galois extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Then, by the Galois correspondence theorem, $F/\mathbb{Q}$ is Galois with Galois group given by H/N. Since $\mathbb{Z}_{p_i-1}/N_i \cong \mathbb{Z}_{n_i}$, we have that $H/N \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} = G$. Thus we obtain the desired result.

(b) By Dirichlet theorem, there are infinitely many primes p such that $p - 1 \in (n_i)$. Therefore we can create a family $\mathcal{F} = \{S_i \mid i \in \mathbb{N}\}$ with $S_i = \{p_{i1}, \dots, p_{ik}\}$ such that the p_{ij}'s are prime satisfying $p_{ij} - 1 \in (n_j)$ and $S_r \cap S_t$ is empty for $r \neq t$. Define $c_i = \Pi_{j=1}^k p_{ij}$ for all $i \in \mathbb{N}$. Now consider the extensions $\mathbb{Q}(\zeta_i)$ of $\mathbb{Q}$ where ζ_i is a primitive c_i^{th}-root of unity. Since $(c_r, c_t) = 1$ for $r \neq t$, we have that $\mathbb{Q}(\zeta_i) \cap \mathbb{Q}(\zeta_j) = \mathbb{Q}$. For each i we generate, similarly as we did in part (a), an intermediate field F_i whose Galois group is G. Since $[k : \mathbb{Q}] < \infty$ and $\mathbb{Q}(\zeta_i) \cap \mathbb{Q}(\zeta_j) = \mathbb{Q}$ for all $i \neq j$, there are at most finitely many i's such that $\mathbb{Q}(\zeta_i) \cap k$ strictly contains $\mathbb{Q}$. Therefore, for the infinitely many i's satisfying $F_i \cap k = \mathbb{Q}$,

$$Gal(kF_i/k) \approx Gal(F_i/\mathbb{Q}) \approx G.$$

■

Problem 39. *(Lang VI.24) Prove that there are infinitely many non-zero relative prime integers a, b such that $-4a^3 - 27b^2$ is a square in $\mathbb{Z}$.*

Solution: (kindly provided by my professor Vera Serganova.) We can do it in the following way. We want $d^2 = -4a^3 - 27b^2$ or, equivalently, $a^3 = (d^2 + 27b^2)/4$. We note that the right hand side is the norm of $(d+3b\sqrt{-3})/2$ in the field $\mathbb{Q}(\omega)$, where ω is a primitive third root of unity. For any $\alpha \in \mathbb{Z}[\omega]$, the norm of α^3 is the cube of the norm of α. Since the norm of α is integral, we can take any α and set $\alpha^3 = (d + 3b\sqrt{-3})/2$ and then a is the norm of α. To make a and b relatively prime, we can take for example $\alpha = (1 + 3p\sqrt{-3})/2$ with p prime. Then b and d are relatively prime, and hence so are a and b.

■

Problem 40. *(Lang VI.31) Let F be a finite field and K a finite extension of F. Show that the norm N_F^K and the trace T_F^K are surjective (as maps from K into F).*

Solution: Let p be the characteristic of F. We write T_F^K and N_F^K simply as T and N, respectively. First we prove that the trace is surjective. Since $T\colon K \to F$ is a linear transformation of vector spaces over F, and F has dimension 1, we have that $\operatorname{Im}(T)$ is either 0 or F. Since K/F is a finite Galois extension, its Galois group G is finite. Therefore, by Artin theorem, the elements of G must be linearly independent. This implies that there is $a \in K^\times$ such that $T(a) \neq 0$. Hence $\operatorname{Im}(T) = F$.

Now we prove that N is surjective. Suppose that $|K| = p^n$. The extension K/F is Galois because K/F is finite and separable. Let G be the Galois group of K/F. Since every finite extension of a finite field is cyclic, there exists $\phi \in G$ such that $G = \langle \phi \rangle$. On the other hand, the groups of units K^* and F^* of K and F are cyclic. Since N is multiplicative, it induces a group homomorphism $L_N\colon K^* \to F^*$ given by $L_N(a) = N(a)$. An element $a \in K^*$ is in $\ker(L_N)$ if and only if

$$1 = \prod_{i=0}^{n-1} \phi^i(a) = \prod_{i=0}^{n-1} a^{p^i} = a^{1+p+\cdots+p^{n-1}}.$$

This happens if and only if a is a root of the polynomial $p(x) = x^c - 1$ where $c = 1 + p + \cdots p^{n-1}$. Therefore $|\ker(L_N)| = c$, and so

$$|K^*/\ker(L_N)| = \frac{p^n - 1}{c} = p - 1.$$

By the first isomorphism theorem, $|\operatorname{Im}(L_N)| = p - 1$. Hence L_N is surjective and then so is N.

■

Problem 41. *(Hungerford V.8.9) If $n > 2$ and ζ is a primitive n-th root of unity over $\mathbb{Q}$, then $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$.*

Solution: Denote by K the field $\mathbb{Q}(\zeta + \zeta^{-1})$. Let G be the Galois group of the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Let $\sigma \in G$ be the conjugation automorphism. Consider the cyclic subgroup $\langle \sigma \rangle$ of G. We shall prove that K is the fixed field of $\langle \sigma \rangle$. It is easy to see that σ fixes K. Suppose that $\phi \in G$ fixes $\zeta + \zeta^{-1}$. Then

$$\zeta + \zeta^{-1} = \phi(\zeta + \zeta^{-1}) = \phi(\zeta) + \phi(\zeta)^{-1}.$$

Since ζ is primitive, $\phi(\zeta) = \zeta^i$ for some i. Substituting $\phi(\zeta) = \zeta^i$ conveniently in the above expression, we obtain $\zeta(\zeta^{i+1} - 1)(\zeta^{i-1} - 1) = 0$. Therefore i is either $1 \pmod{\varphi(n)}$ or $-1 \pmod{\varphi(n)}$. Hence K is the fixed field of $\langle \sigma \rangle$. Then, by the Galois correspondence theorem, $[\mathbb{Q}(\zeta) : K] = 2$. This implies that

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]/[\mathbb{Q}(\zeta) : K] = \varphi(n)/2.$$

■

Problem 42. *(Hungerford V.8.9) Let p be prime and ζ be a primitive p-th root of unity. Find all subfields $F \subseteq \mathbb{Q}(\zeta)$ such that $[F : \mathbb{Q}] = 2$.*

Solution: The Galois group G of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. Since G is cyclic and $|G| = p-1$, it contains only one subgroup H of order $\frac{p-1}{2}$. This implies, by the Galois correspondence theorem, that there is only one intermediate field F of $\mathbb{Q}(\zeta)/\mathbb{Q}$ such that $[F : \mathbb{Q}] = 2$, namely the fixed field of H. Since H is a cyclic group, we can write $H = \langle \sigma \rangle$ where $\sigma \in H$. If $\tau = T_F^{\mathbb{Q}(\zeta)}(\zeta) \in F$ then $\mathbb{Q}(\tau) \subseteq F$. Now suppose that $\rho \in G$ fixes τ. Since $\zeta, \dots, \zeta^{p-1}$ form a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, τ can be written uniquely as a linear combination of the ζ^i's. The fact that ρ fixes τ implies that $\rho(\zeta) = \sigma^j(\zeta)$ for some j. Consequently $\rho = \sigma^j \in H$. Hence we can conclude that $F = \mathbb{Q}(\tau)$ is the only intermediate field of degree 2 over $\mathbb{Q}$.

■

Problem 43. *Show that any finite group is isomorphic to the Galois group of some finite extension $F \subseteq E$.*

Solution: Suppose that G is a finite group of order n. The action of G on itself by left multiplication induces a homomorphism $f \colon G \to S_n$. Since f is injective we can think of G as a subgroup of S_n. Also, we have seen that for each n the symmetric group S_n is the Galois group of a field extension E/F. Since G is a subgroup of S_n, by the Galois correspondence, there exists an intermediate field K of the extension E/F such that $Gal(E/K)$ is isomorphic to G.

■

Problem 44. *Let $\bar{\mathbb{Q}} \subset \mathbb{C}$ denote the subfield of algebraic numbers and G be the (infinite) Galois group of $\bar{\mathbb{Q}}$ over $\mathbb{Q}$. We call $\alpha \in \bar{\mathbb{Q}}$ totally real if $g(\alpha) \in \mathbb{R}$ for any $g \in G$.*
(a) Prove that the set H of all totally real elements is a subfield of $\bar{\mathbb{Q}}$.
(b) Is the field extension $H/\mathbb{Q}$ normal?

Solution: (a) Suppose that $\alpha, \beta \in H$. For any $g \in G$ $g(0) = 0 \in \mathbb{R}$ and $g(\alpha + \beta) = g(\alpha) + g(\beta) \in \mathbb{R}$. Also, $g(1) = 1$ and, if $\beta \neq 0$, $g(\alpha\beta^{-1}) = g(\alpha)g(\beta)^{-1} \in \mathbb{R}$. Therefore H is a subfield of $\bar{\mathbb{Q}}$.

(b) Suppose that $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial with splitting field $F \subset \bar{\mathbb{Q}}$. Let α be a root of $f(x)$ in H. Let $\beta \in F$ be another root of $f(x)$. Since $f(x)$ is irreducible, $G_F = Gal(F/\mathbb{Q})$ acts transitively on the roots of f. Then there exists $\sigma \in G_F$ such that $\sigma(\alpha) = \beta$. Since any automorphism of F extends to its algebraic closure $\bar{\mathbb{Q}}$, there exists $\bar{\sigma} \in G$ such that $\bar{\sigma}|_F = \sigma$. Now suppose that g is an arbitrary element of G. Then $g(\beta) = (g \circ \bar{\sigma})(\alpha) \in \mathbb{R}$; this is because $g \circ \bar{\sigma} \in G$ and $\alpha \in H$. Therefore $\beta \in H$. Hence all roots of $f(x)$ are in H. Since $f(x)$ was arbitrarily taken, $H/\mathbb{Q}$ is a normal extension.

■

Problem 45. *Let p be a prime number and F be the splitting field for the family of polynomials $x^{p^r} - 1$ for all $r > 0$. Prove that the Galois group of F over $\mathbb{Q}$ is isomorphic to the inverse limit $\varprojlim_r (\mathbb{Z}/p^r\mathbb{Z})^\times$.*

Solution: The splitting field of $p_r(x) = x^{p^r} - 1$ is $F_r = \mathbb{Q}(\zeta_r)$ where ζ_r is a primitive p^rth root of unity. Therefore $F = \mathbb{Q}(\zeta_1, \zeta_2, \dots)$. Since each ζ_i is separable over $\mathbb{Q}$ so is F. Then $F/\mathbb{Q}$ is a Galois extension. Let G be the Galois group of the extension $F/\mathbb{Q}$ and $G_r \approx (\mathbb{Z}/p^r\mathbb{Z})^\times$ be the Galois group of the extension $F_r/\mathbb{Q}$.

For $j \geq i$ we define $q_i^j \colon G_j \to G_i$ by $q_i^j(\sigma) = \sigma|_{F_i}$. Then (G_i, q_i^j) is a directed family of groups. Let $\bar{G}$ be its inverse limit. We show that $\bar{G}$ is isomorphic to G. Define the map $f \colon G \to \bar{G}$ by $f(\sigma) = (\sigma|_{F_r})$. Since $q_i^j(\sigma|_{F_j}) = \sigma|_{F_i}$ for $j \geq i$, the map f is well defined. Also f is a homomorphism.

We show that f is injective. If $\sigma \in \ker(f)$ then $\sigma|_{F_r}$ is the identity for any $r > 0$. Since $F = \cup F_r$, for each $x \in F$ there exists r such that $x \in F_r$. So $\sigma(x) = \sigma|_{F_r}(x) = x$. Hence f is injective. Now take $(\sigma_r) \in \bar{G}$. Define $\sigma \in G$ as follows. For $x \in F$ take r such that $x \in F_r$, and set $\sigma(x) = \sigma_r(x)$. Suppose that $x \in F_i$ and $x \in F_j$ for $i \leq j$. Since $(\sigma_r) \in \bar{G}$, $\sigma_j|_{F_i} = \sigma_i$. So $\sigma(x)$ does not depends on the choice of r. Since $F_1, F_2, \dots$ is an increasing sequence of fields whose union is F, the fact that $f|_{F_r}$ is an automorphism for each $r > 0$ implies that σ is an automorphism of F. Since $\sigma \in G$ and $f(\sigma) = (\sigma_r)$, the homomorphism f is surjective. Hence f is an isomorphism, which implies that

$$Gal(F/\mathbb{Q}) = G \approx \varprojlim_r G_r = \varprojlim_r (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

■

6 Further Problems

Problem 46. *Prove the following statements.*
(a) The group of rotational symmetries of the icosahedron is isomorphic to A_5.
(b) $PSL(2, \mathbb{F}_5) \cong A_5$.

Problem 47. *Consider all ideals of $\mathbb{Z}$ as forming a directed system, by divisibility. Prove that*

$$\varprojlim_{(a)} \mathbb{Z}/(a) = \prod_p Z_p,$$

where the limit is taken over all ideals (a), and the product is taken over all prime p.

Problem 48. *Find a ring R such that R is not isomorphic to R^{op}.*

Problem 49. *Let k be a field, G be a finite group, and $k[G]$ denote the group ring.*
(a) Show that any finitely generated $k[G]$-module is finite-dimensional over k.
(b) Show that any finite dimensional projective module is injective.

Problem 50. *(Lang III.25) Show that any module is a directed limit of finite presented modules.*

Problem 51. *(Lang III.26) Let E be a module over a ring. Let (M_i) be a directed family of modules. If E is finitely generated, show that the natural homomorphism*

$$\varinjlim \mathrm{Hom}(E, M_i) \to \mathrm{Hom}(E, \varinjlim M_i)$$

is injective. If E is finitely presented, show that this homomorphism is an isomorphism.