Chapter 2 - Groups I

Exercise 1. Let G be a group of order 1210.

a) Prove that G has a normal subgroup of order 121 that is abelian.

We are going to use the Sylow theorem:

2.7.2 Theorem: Let p be a prime. Let G be a finite group. Let p^e be the largest power of p dividing the order of G. Then
- G has p-Sylow subgroups.
- Every subgroup of G with order a power of p lies inside a p-Sylow subgroup of G.
- The number n_p of p-Sylow subgroups satisfies

$$n_p | \text{order}(G) \qquad n_p = 1 \bmod p$$

- Any two p-Sylow subgroups P and Q are **conjugate**. [17]
- A group of order p^n has a non-trivial center.

$\text{order}(G) = 121 = 2 \cdot 5 \cdot 11^2$

$n_{11} = 1, 2, 5, 10$ because $n_{11} | \text{order}(G)$

$2 \neq 1 \mod 11 \quad 5 \neq 1 \mod 11 \quad 10 \neq 1 \mod 11$

So we conclude that there only exists one 11-Sylow subgroup ($n_{11} = 1$). Being the only one 11-Sylow subgroup implies that it is a normal subgroup in G. This subgroup has order 121, which is $11^2 = p^2$ ($p = 11$). Since 11 is prime, we know that groups with order a prime squared are abelian, so the 11-Sylow subgroup is abelian. From now on, we'll call this subgroup N.

b) Prove that N has a normal cyclic subgroup of order 11 and G/N has a normal subgroup of order 5.

The order of N is 11^2. We also know that N is abelian. We will use the following lemma:

2.7.3 Lemma: Let A be a finite *abelian* group, and let p be a prime dividing the order of A. Then there is an element a of A of order exactly p. Thus, there exists a subgroup of A of order p.

Because of this lemma, we know that in N there exists an element of order 11 and therefore, a subgroup of order 11 (the one that is generated by that element, meaning that it is cyclic). Every subgroup in N is normal because N is abelian, so we have found a normal cyclic subgroup of order 11 in N. Now, let's consider the quotient group G/N:

$$\left|G/N\right| = [G:N] = \frac{|G|}{|N|} = \frac{1210}{121} = 10 = 2 \cdot 5$$

$n_5 = 1, 2$ but $2 \neq 1 \bmod 5$ so $n_5 = 1$

There is only one 5-Sylow subgroup in G/N, so it is a normal subgroup of order 5.

Exercise 2. Consider a finite group G and d a divisor of the order of G. There only exists a subgroup H of order d. Prove that H is a normal subgroup of G.

Let's consider a random element $h \in H$ and a random element $g \in G$:

$$(ghg^{-1})^d = \underbrace{ghg^{-1} \cdot \ldots \cdot ghg^{-1}}_{d \text{ times}} = gh^d g^{-1} = gg^{-1} = 1$$

The order of h divides the order of the group where it belongs

Since the above holds for all $h \in H$, the subgroup gHg^{-1} has order d. H is the only subgroup of order d, so $gHg^{-1} = H$. Then every $h \in H$ has some $h' \in H$ such that $ghg^{-1} = h'$, implying $gh = h'g$, so $gH = Hg$, which means that H is a normal subgroup.

Chapter 6 - Fields I

6.3 Find a polynomial with rational coefficients having a root $\sqrt{2}+\sqrt{3}$.

First, we will find a polynomial with root $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$

$$x-(\sqrt{2}+\sqrt{3})=0 \iff x-\sqrt{2}-\sqrt{3}=0$$

We isolate the squared root of 3 and we square both sides:

$$(x-\sqrt{2})^2=(\sqrt{3})^2 \iff x^2-2\sqrt{2}x+2=3 \iff \underbrace{x^2-2\sqrt{2}x-1=0}$$

Polynomial in $\mathbb{Q}(\sqrt{2})$ with $\sqrt{2}+\sqrt{3}$ as a root

Now we isolate the square roots of 2 and square both sides again:

$$(x^2-1)^2=(2\sqrt{2}x)^2$$

$$x^4-2x^2+1=8x^2$$

$$\underbrace{x^4-10x^2+1=0}$$

$q(x)$ is the polynomial we were looking for

Find a polynomial with rational coefficients having a root $\sqrt{3}+\sqrt[3]{6}$.

First, we will find a polynomial with root $\sqrt{3}+\sqrt[3]{6}$ over $\mathbb{Q}(\sqrt{3})$:

$$x-(\sqrt{3}+\sqrt[3]{6})=0 \iff x-\sqrt{3}-\sqrt[3]{6}=0$$

We isolate the cubic root and we elevate both sides to the power of 3:

$$(x-\sqrt{3})^3=(\sqrt[3]{6})^3 \iff x^3-3\sqrt{3}x^2+9x-3\sqrt{3}=6$$

Now we isolate the square roots of 3 and square both sides:

$$(x^3+9x-6)^2=(3\sqrt{3}x^2+3\sqrt{3})^2$$

$$x^6+18x^4-12x^3+81x^2-108x+36=27x^4+54x^2+27$$

$$\underbrace{x^6-9x^4-12x^3+27x^2-108x+9}_{p(x)}=0$$

$p(x)$ is the polynomial we were looking for

6.5 Let γ be a root of $x^5 - x + 1 = 0$ in an algebraic closure of $\mathbb{Q}$. Find a polynomial with rational coefficients of which $\gamma + \sqrt{2}$ is a root.

$\alpha = \gamma + \sqrt{2}$

$\gamma = \alpha - \sqrt{2}$

We know that γ is a root of $x^5 - x + 1$, so we have:

$(\alpha - \sqrt{2})^5 - \alpha + \sqrt{2} + 1 = 0$

$\alpha^5 - 5\sqrt{2}\alpha^4 + 20\alpha^3 - 20\sqrt{2}\alpha^2 + 20\alpha - 4\sqrt{2} - \alpha + \sqrt{2} + 1 = 0$

$\alpha^5 + 20\alpha^3 + 19\alpha + 1 = 5\sqrt{2}\alpha^4 + 20\sqrt{2}\alpha^2 + 3\sqrt{2}$

$\alpha^5 + 20\alpha^3 + 19\alpha + 1 = (5\alpha^4 + 20\alpha^2 + 3)\sqrt{2}$

Now, we square both sides:

$\alpha^{10} + 40\alpha^8 + 438\alpha^6 + 2\alpha^5 + 760\alpha^4 + 40\alpha^3 + 361\alpha^2 + 38\alpha + 1 =$

$50\alpha^8 + 400\alpha^6 + 860\alpha^4 + 240\alpha^2 + 18$

$\alpha^{10} - 10\alpha^8 + 38\alpha^6 + 2\alpha^5 - 100\alpha^4 + 40\alpha^3 + 121\alpha^2 + 38\alpha - 17 = 0$

This is the polynomial we were looking for

Chapter 7 - Some Irreducible Polynomials

7.5 Show that the ideal generated by $x^2 - x + 1$ and 13 in $\mathbb{Z}[x]$ is *not* maximal.

We are going to consider the quotient ring $\mathbb{Z}[x]/I$ with I being the ideal generated by 13 and x^2-x+1. Because of example 7.2.3, we know that we can compute the quotient in two steps:

$$\mathbb{Z}[x]/\langle 13\rangle \cong \mathbb{Z}_{13}[x]$$

In $\mathbb{Z}_{13}[x]$, the polynomial x^2-x+1 does factor, as:

$$x^2-x+1 = x^2+12x+1 = (x+3)(x+9)$$

meaning that x^2-x+1 is not irreducible in $\mathbb{Z}_{13}[x]$.

Thus, the quotient $\mathbb{Z}_{13}[x]/\langle x^2-x+1\rangle$ has proper zero divisors $\overline{x}+3$ and $\overline{x}+9$, where $\overline{x}$ is the image of x in the quotient. Thus, $\mathbb{Z}[x]/I$ is not an integral domain, much less a field, so I is not maximal because of the following result that we have seen in class:

4.5.1 Proposition: For a commutative ring R with unit, and for an ideal I, the quotient ring R/I is a *field* if and only if I is a *maximal* ideal.

Chapter 10 - Modules over PIDs

Count the number of abelian groups of order 1800.

Since $1800 = 2^3 \cdot 3^2 \cdot 5^2$, every abelian group of order 1800 is uniquely expressible as a direct sum of an abelian group of order 2^3, an abelian group of order 3^2 and an abelian group of order 5^2. Now using the corollary 10.3.3, the number of abelian groups of order p^n for any p prime is the number of sums of non-decreasing sequences of positive integers which sum to the exponent n. We have to study two cases:

•) $n = 2 \Rightarrow$ Here we only have two possibilities:

$$1 + 1 = 2$$
$$2 = 2$$

That is, the abelian groups of order p^2 for prime p are:

$$\mathbb{Z}_p \oplus \mathbb{Z}_p$$
$$\mathbb{Z}_{p^2}$$

•) $n = 3 \Rightarrow$ Here we have three possibilities:

$$1 + 1 + 1 = 3$$
$$1 + 2 = 3$$
$$3 = 3$$

That is, the abelian groups of order p^3 for prime p are:

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$$
$$\mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$$
$$\mathbb{Z}_{p^3}$$

Thus, there are 3 abelian groups of order 2^3, 2 of order 3^2 and 2 of order 5^2, so we have $3 \cdot 2 \cdot 2 = 12$ ab. groups of order 1800.