The solutions to the book
"Abstract Algebra Theory and Applications"
by Thomas W. Judson

Jian Li
Computer Science
Nanjing University, China

2011

1 Preliminaries

2 The Integers

Problem 16

Suppose a and b are not relatively prime, there exist a k such that $k|a$, $k|b$ and $k \neq 1$. Therefore, we have

$$ar + bs = kpr + kqs = k(pr + qs) = 1$$

So we have $k|1$. It is controdict $k \neq 1$. So a and b are relateively prime.

Problem 28

This problem equivalent the problem "Let $p \geq 2$, if p is not prime, so is $2^p - 1$" Since p is not prime, there exist $k \neq 1$ such that $k|p$. Now we can think that $2^p - 1 = (111...1)_2$, a p-bit binary number. Therefore, we have $2^k - 1|2^p - 1$, since $(\underbrace{111...1}_{k\text{-bits}})|(\underbrace{111...1}_{p\text{-bits}})$. So $2^p - 1$ is not a prime.

3 Groups

Problem 24

Proof:

$$(aba^{-1})^n = aba^{-1}aba^{-1}...aba^{-1} = ab(a^{-1}a)b(a^{-1}a)b...(a^{-1}a)ba^{-1} = ab^na^{-1}$$

Problem 30

Since $a^2 = e$ for all $a \in G$, we have $a = a^{-1}$ for all $a \in G$. For any $a, b \in G$,

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

Therefore, G is an abelian group.

4 Cyclic Groups

Problem 29

Since the number of generators of $\mathbf{Z}_n$ is $\phi(n)$, and $\phi(nm) = \phi(n)\phi(m)$, we have $\phi(m^k) = m^k - m^{k-1}$ for any prime k. Therefore, $\phi(n)$ is even for all $n \geq 3$ and $\mathbf{Z}_n$ has an even number of generators for $n > 2$.

Problem 30

Suppose that there exist $p < m$, $q < n$ such that $a^p = b^q \neq e$, we have $b^{qm} = a^{pm} = e = b^n$. Since $|b| = n$, we conclude that $n|qm$. And we can also conclude that $m|pn$ in the same way. It controdicts gcd(m,n) $= 1$. Thus, $\langle a \rangle \cup \langle b \rangle = \{e\}$.

Problem 36

Since $\mathbf{Z}_n$ is a cyclic group of order n and 1 is a generator of the group. According to Theorem 4.6, we have the order of r is $n/gcd(r,n)$. Since r is a generator, therefore $gcd(r,n) = 1$.

5 Permutation Group

Problem 27

One-to-One:
If $\lambda_g(a) = \lambda_g(b)$, we have $\lambda_g(a) = ga = gb = \lambda_g(b)$, which means $a = b$.
Onto:
For any $b \in G$, we can find that $\lambda_g(g^{-1}b) = gg^{-1}b = b$ and $g^{-1}b \in G$.

Therefore, λ_g is a permutation of G.

Problem 31

Reflexive:
Since $e \in S_n$, we know that $e\alpha e^{-1} = \alpha$ for all $\alpha \in S_n$. Thus, we have $\alpha \sim \alpha$.
Symmetric:
If there exist $\alpha \sim \beta$, it means that $\sigma\alpha\sigma^{-1} = \beta$ for some $\sigma \in S_n$. Then, we have $\alpha = \sigma^{-1}\beta\sigma = \sigma^{-1}\beta(\sigma^{-1})^{-1}$. Thus, we conclude that $\beta \sim \alpha$.
Transitive:
Suppose that we know that $\alpha \sim \beta$ and $\beta \sim \gamma$, it means that $\beta = \sigma\alpha\sigma^{-1}$ and $\gamma = \delta\beta\delta^{-1}$ for some $\sigma, \delta \in S_n$. So $\gamma = \delta\sigma\alpha\sigma^{-1}\delta^{-1} = (\delta\sigma)\alpha(\sigma^{-1}\delta^{-1}) = (\delta\sigma)\alpha(\delta\sigma)^{-1}$ for some $\delta\sigma \in S_n$.

Therefore, $\sim$ is an equivalence relation on S_n.

6 Cosets and Lagrange's Theorem

Problem 17

if $a \notin H$, then $a^{-1} \notin H \Rightarrow a^{-1} \in aH = a^{-1}H = bH \Rightarrow \exists h_1, h_2 \in H$ s.t. $a^{-1}h_1 = bh_2 \Rightarrow ab = h_1{h_2}^{-1} \in H$

Problem 18

if $g \in H$, then $gH = Hg = H$; if $g \notin H$, then $gH = Hg = G - H$

7 Introduction to Cryptography